

2024 FALL RELIABILITY SUMMIT

Brian Thiry, Director, Entity Engagement and External Affairs

Michelle Cross, Manager, External Affairs

Sept. 17, 2024



RELIABILITY FIRST

FERC TRANSMISSION REFORM

ERIC VANDENBERG

Deputy Director of the Office of Reliability, FERC





Office of Electric Reliability

Eric Vandenberg, Acting Director, Office of Electric Reliability

September 17, 2024

The views expressed in this presentation are my own and do not represent those of the Commission or any individual Commissioner.

Agenda

- Overview of OER
- Recent Reliability Orders
- Order 1920
- Upcoming Technical Conferences
- Questions



OER Performs 5 Key Functions

- Advise on whether to approve, remand or require changes to reliability standards proposed by NERC
 - Oversee compliance with approved standards by users, owners, and operators of the Bulk-Power System (BPS); review NERC-proposed penalties
 - Provide engineering support on rate filings, focusing on potential reliability impacts
 - Monitor the status of the BPS to keep the Commission informed of evolving events
 - Review blackouts and major events for possible violations of, or gaps in, reliability standards
- More info available in [Electric Reliability Primer](#)



Priorities



Cyber and Physical Security

Supply Chain Compromise
Protections for Low Impact Assets
Physical Security



Resource Transition

Inverter Based Resources
Resource/Energy Adequacy
Priority System Attributes (e.g.,
quick start, ramping)



Extreme Weather

Asset Hardening (e.g.,
generator freeze protection)
System Planning and Design



Recent Reliability Orders

- IBR Registration
 - Approved NERC's proposal
 - Category 2 GO/ GOP Compliant by May 2026
- EOP-012-2 (Generator Winterization)
 - Approved, effective October 1
 - Directed further modifications due March 2025
- DLR ANOPR
 - Comments are due October 15, 2024, and reply comments are due November 12, 2024



Order No. 1920

- Conduct long-term transmission planning to account for expected changes in generation and demand
- Consider a required set of minimum benefits when planning new facilities
- Identify opportunities to “right-size” transmission facilities to increase their transfer capability
- Expands states’ pivotal role throughout the process



Recent/ Upcoming Conferences

- [Innovations and Efficiencies in Generator Interconnection Workshop](#)
 - Discussion of opportunities for further innovation and increased efficiency in the generator interconnection process
 - September 10-11, 2024
- [Annual Reliability Tech Conference](#)
 - Discuss policy issues related to the reliability and security of the Bulk-Power System
 - October 16, 2024
- [Co-Location of Large Loads at Generating Facilities](#)
 - Discuss generic issues related to the co-location of large loads at generating facilities
 - November 1, 2024



Questions?



NERC INTERREGIONAL TRANSFER CAPABILITY STUDY UPDATE

JOHN MOURA

Director of Reliability Assessment
and Performance Analysis, NERC



NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Assuring a Reliable BPS through the Expansion of Interregional Transfer Capability: NERC ITCS

John Moura

Director, Reliability Assessment and Performance Analysis

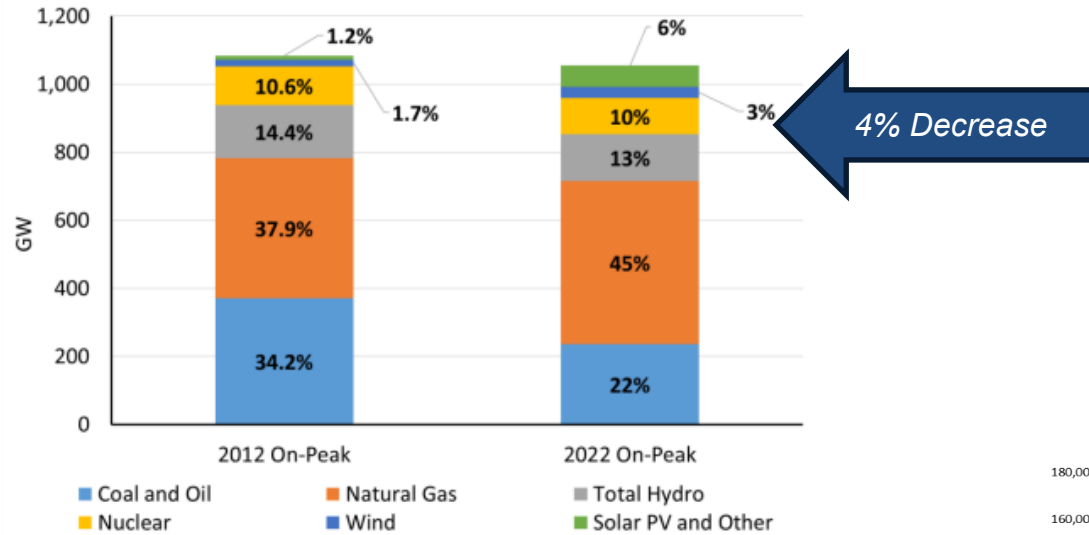
2024 Fall Reliability and Security Summit

September 17, 2024

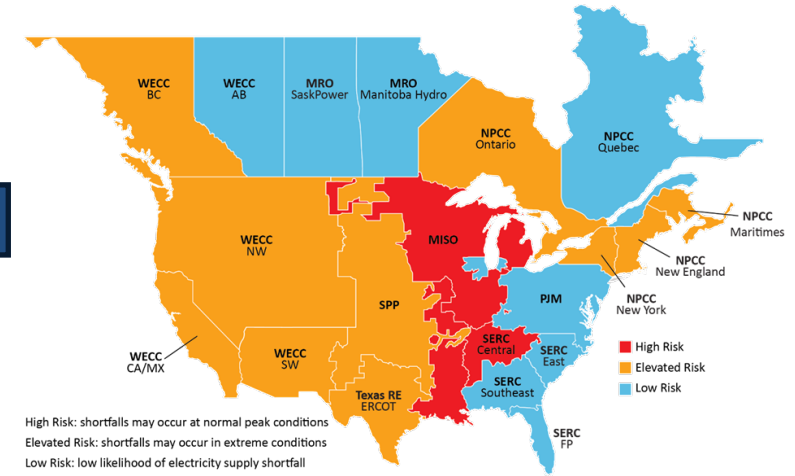
RELIABILITY | RESILIENCE | SECURITY



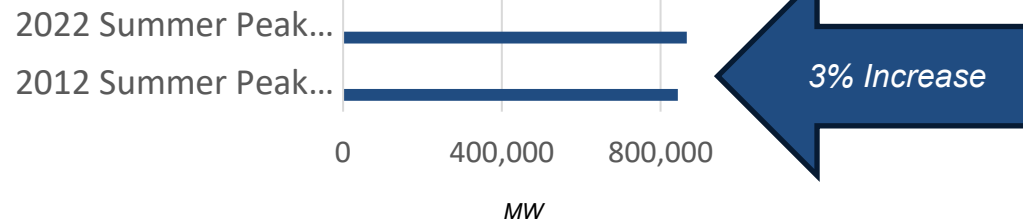
2012 and 2022 Peak Capacity Resource Mix NERC-Wide



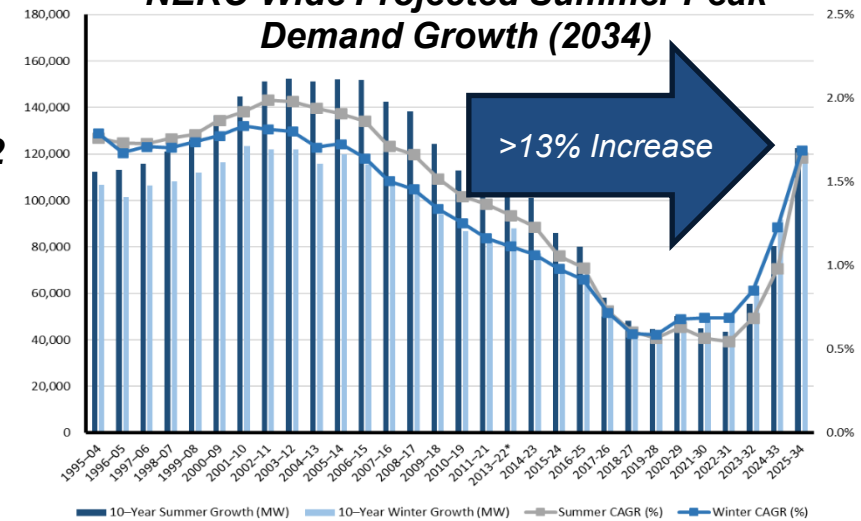
2024-2033 Risk Areas



NERC-Wide Summer Peak Demand Changes 2012 and 2022

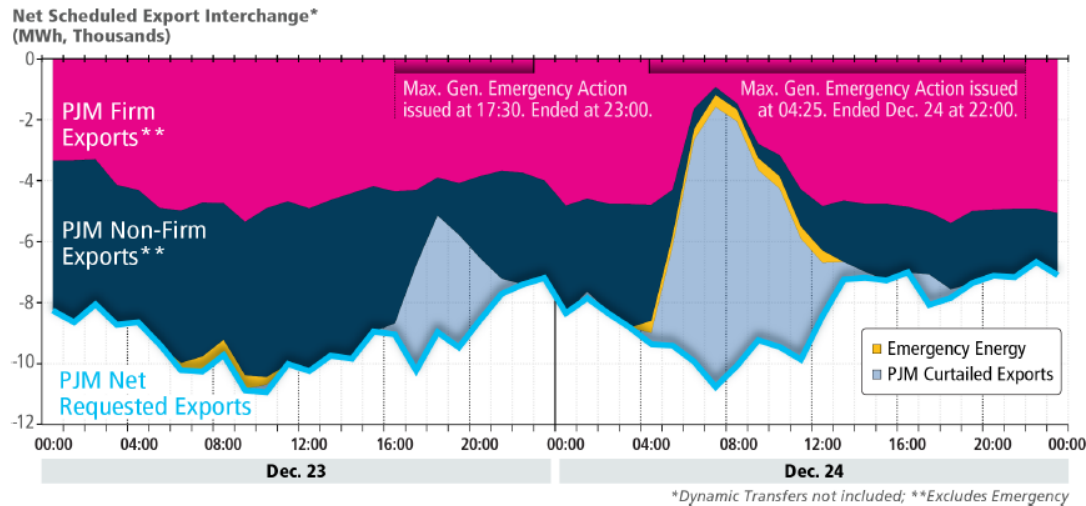
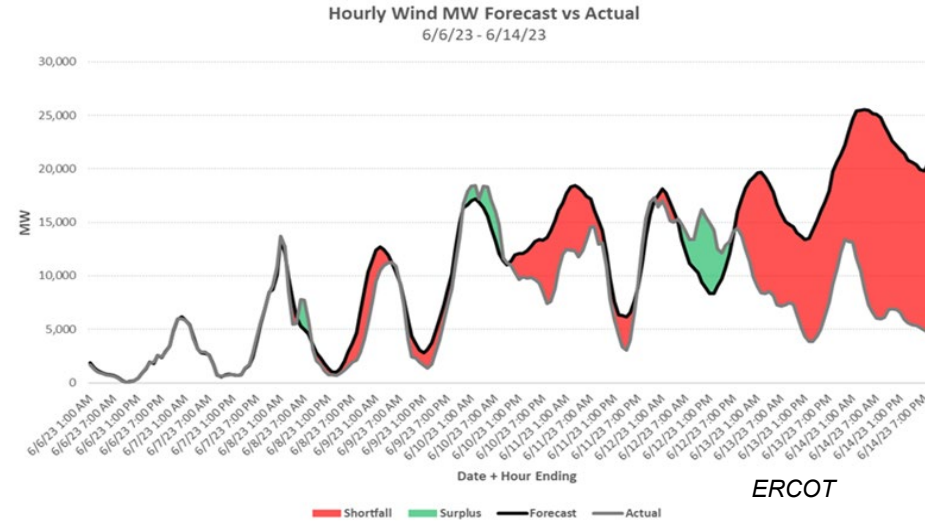


NERC-Wide Projected Summer Peak Demand Growth (2034)



Recent Examples Highlight Need for Wide-Area Energy Assessments

June 6, 2023: ERCOT, SPP, MISO:A
“wind drought” caused 60 GW of
installed wind capacity to generate
300 MW



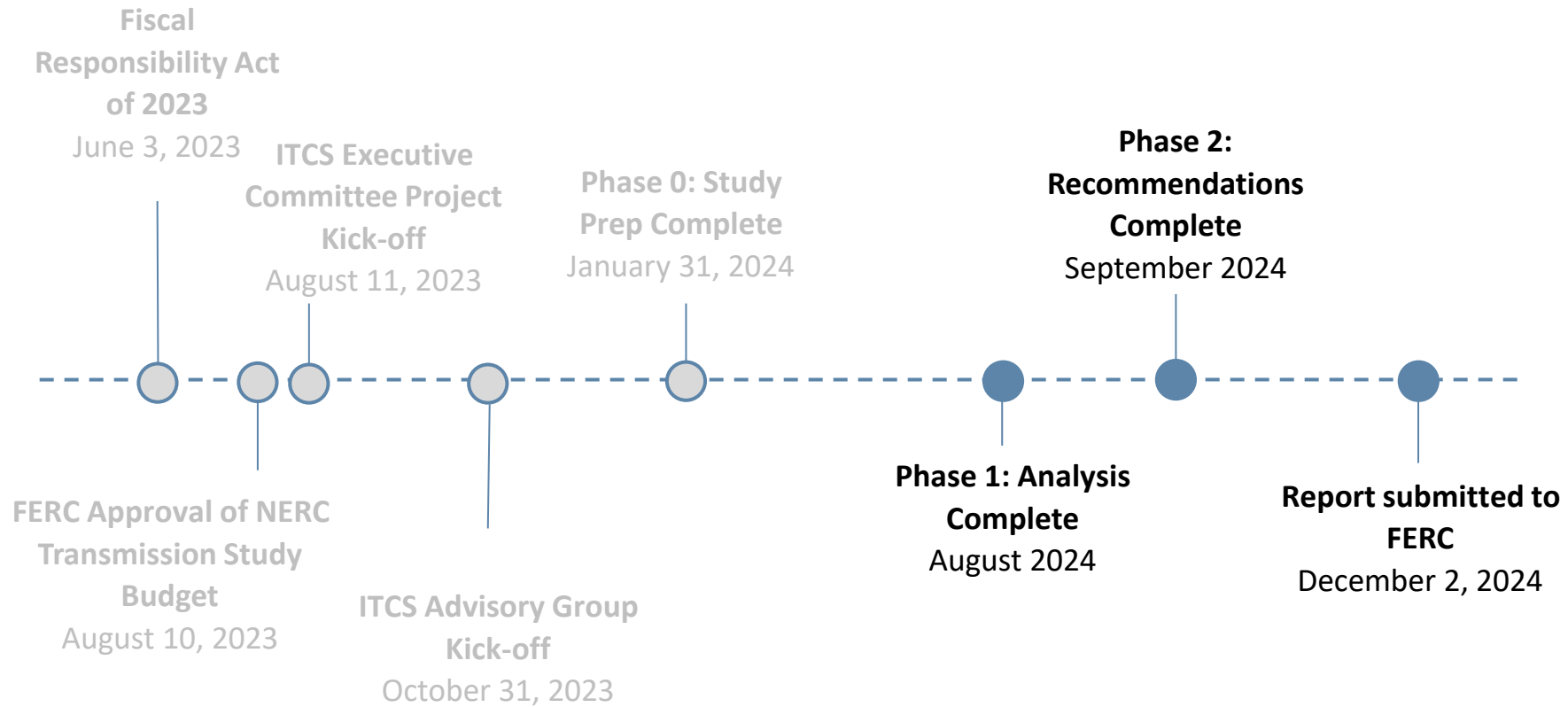
December 24, 2022: PJM:
Transmission system during
extreme cold weather limited the
ability to export to support southern
neighbors



Fiscal Responsibility Act (FRA), Section 322

In consultation with the Regional Entities and transmitting utilities, NERC shall conduct a study containing three elements:

1. **Current total transfer capability**, between each pair of neighboring transmission planning regions.
2. A recommendation of **prudent additions to total transfer capability** between each pair of neighboring transmission planning regions that would demonstrably strengthen reliability within and among such neighboring transmission planning regions.
3. Recommendations on **how to meet and maintain the identified total transfer capability**, together with the prudent recommended additions in #2.





Varies Widely

- Current transfer capability changes (TTC) as percentage of peak load = 1% to 92% between regions, varying greatly depending on season and online generation dispatch



Transmission May Not Always be a Solution

- New transmission will not always increase transfer capability
- Voltage and dynamic stability limitations will determine how much power can be transferred



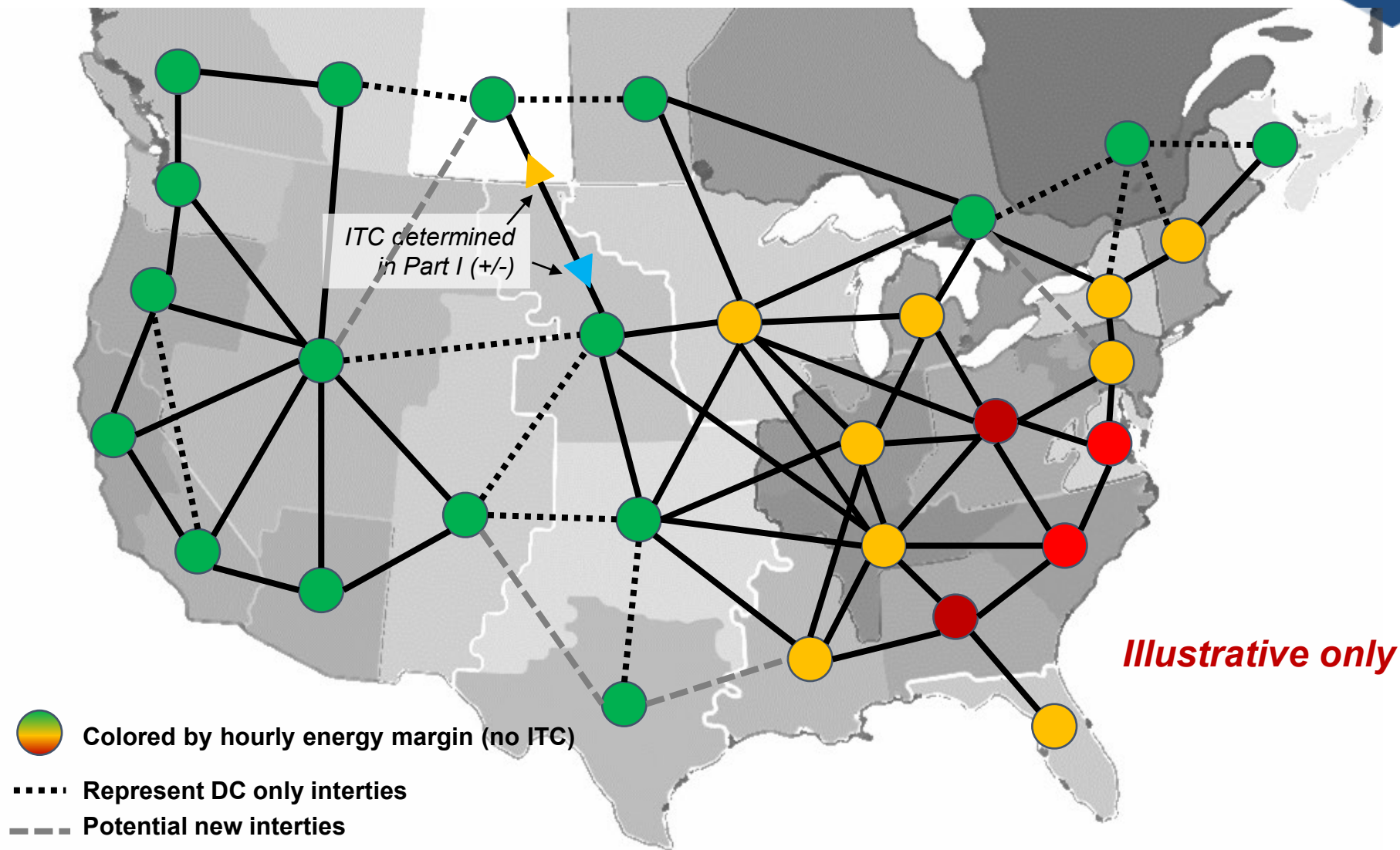
Resource Evaluation Cannot be Overlooked

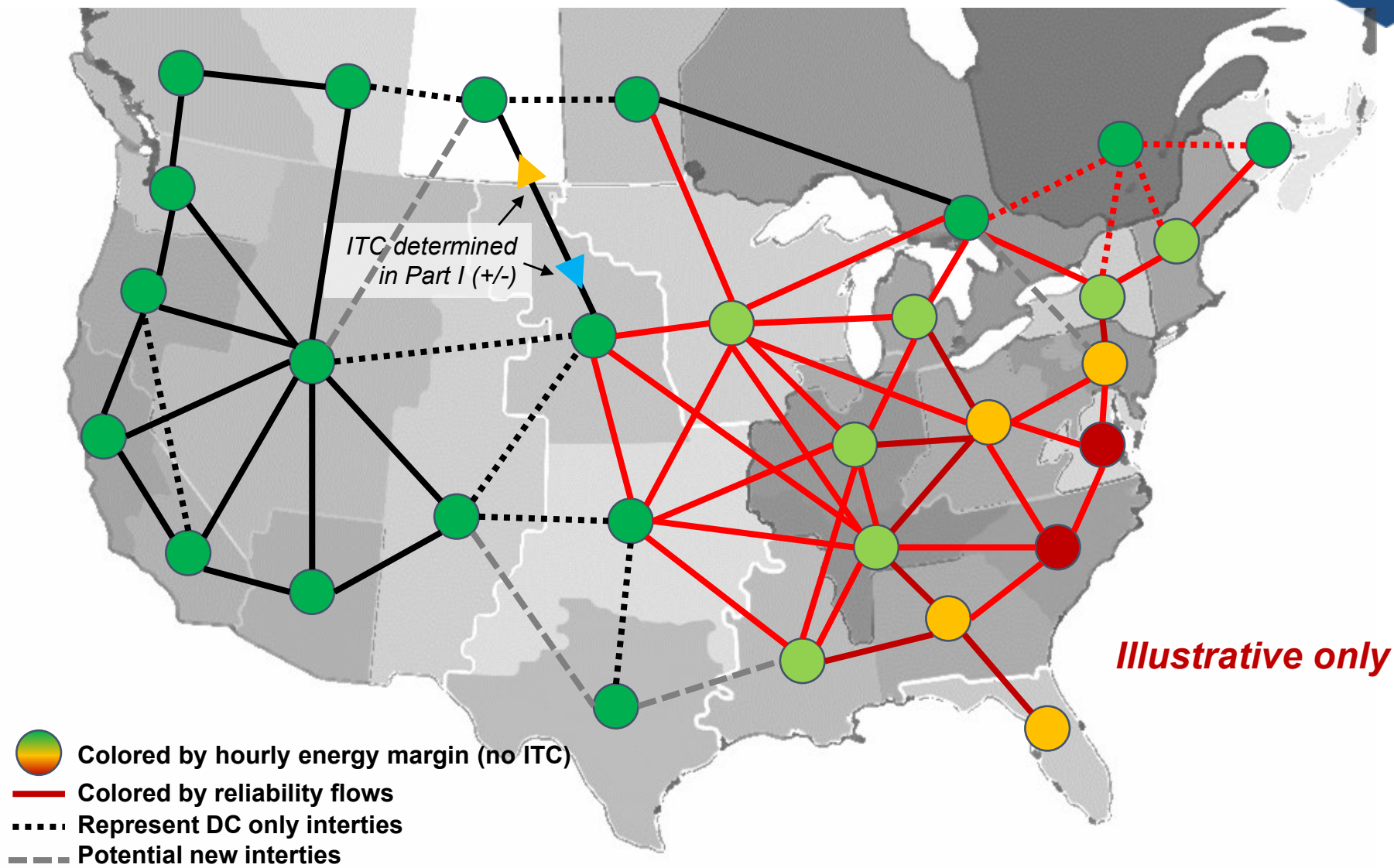
- Many areas do not have sufficient committed generation to meet demand under extreme conditions (2034)
- Canadian system critical to this evaluation



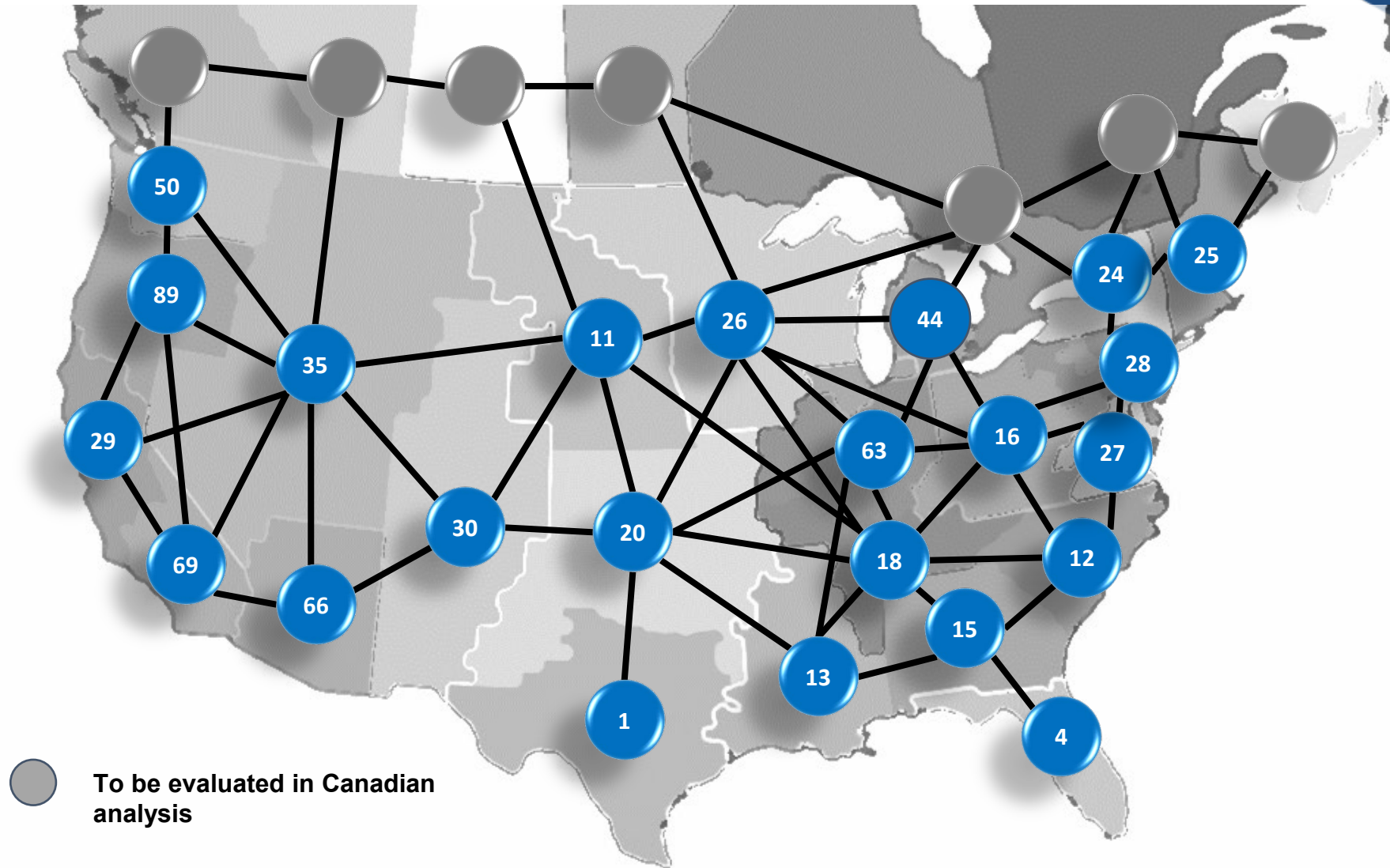
Higher TTCs Will Require Significant Planning and System-Wide Reinforcements

- TTC additions will require more granular stability studies once specific projects are evaluated
- Meaningful TTC additions will not be completed by 2034 without regulatory/legislative changes

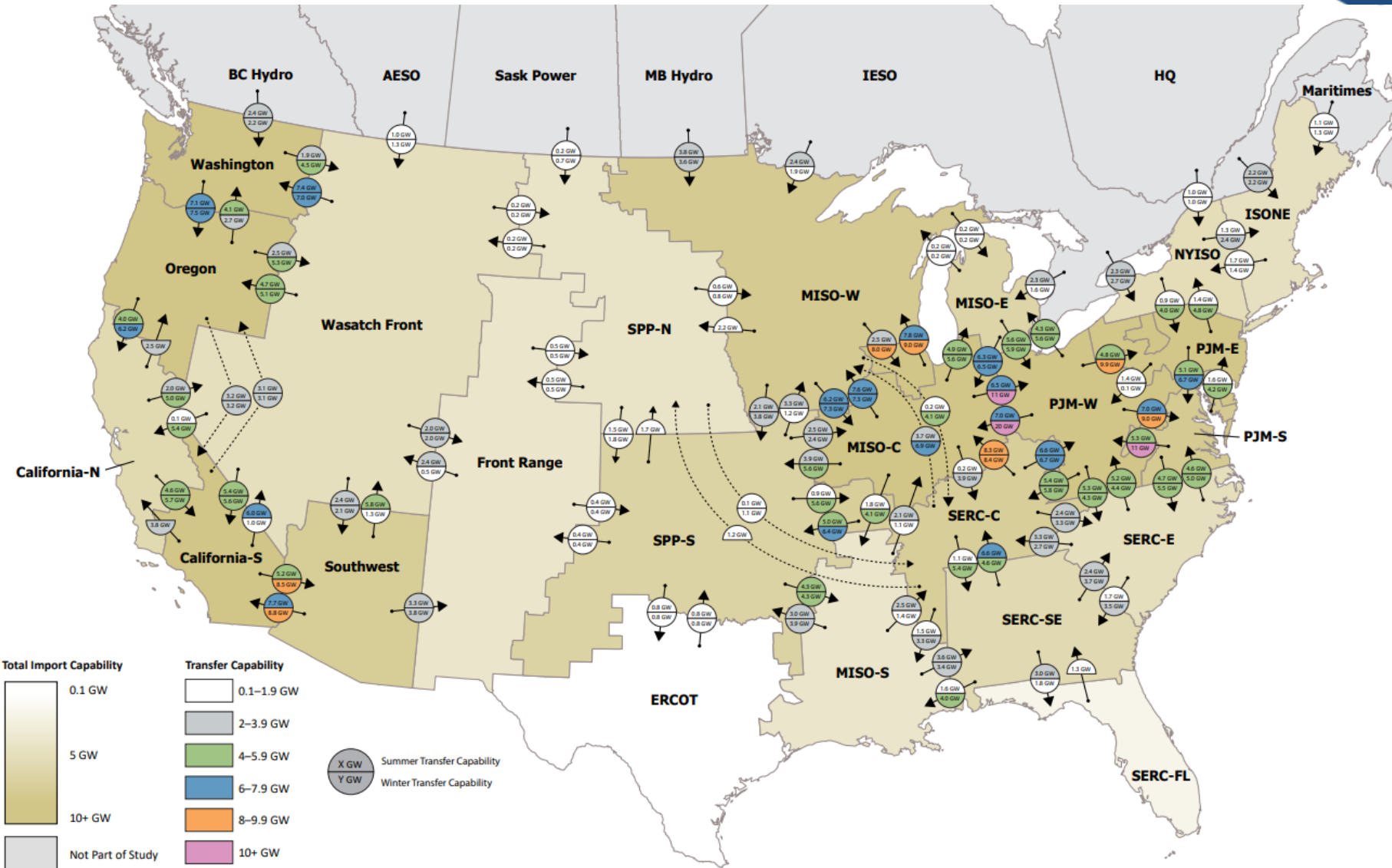


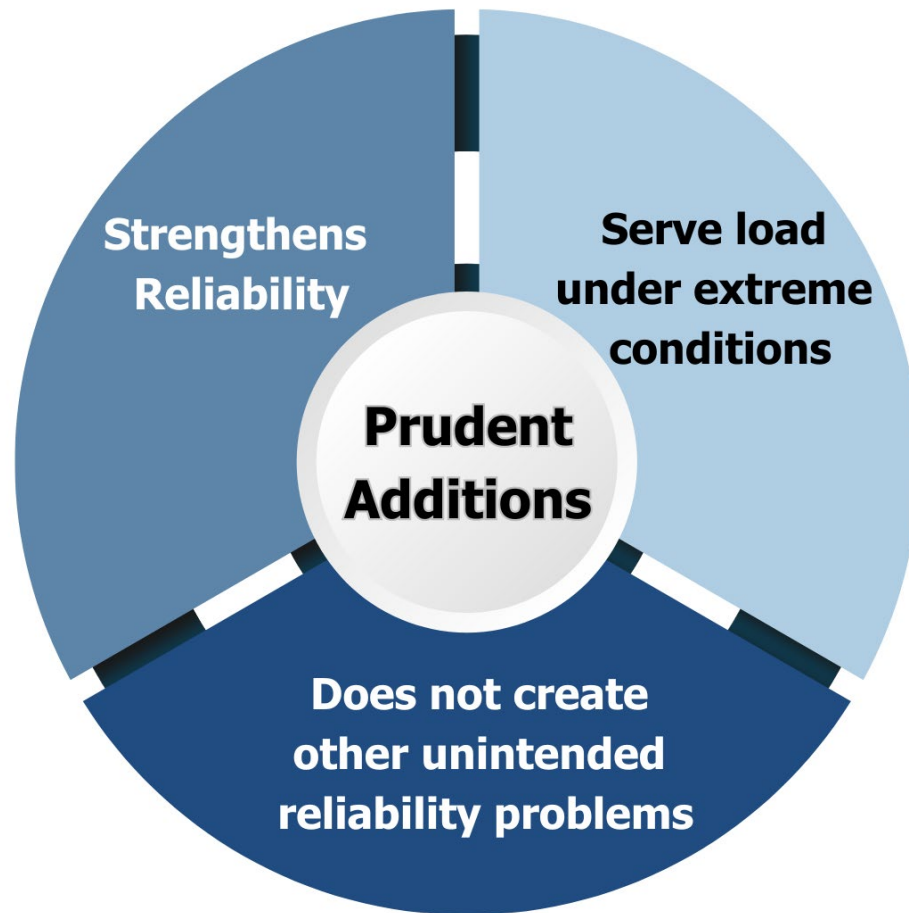


Part I Total Import Capabilities as Percentage of 2024 Peak Load (Winter)

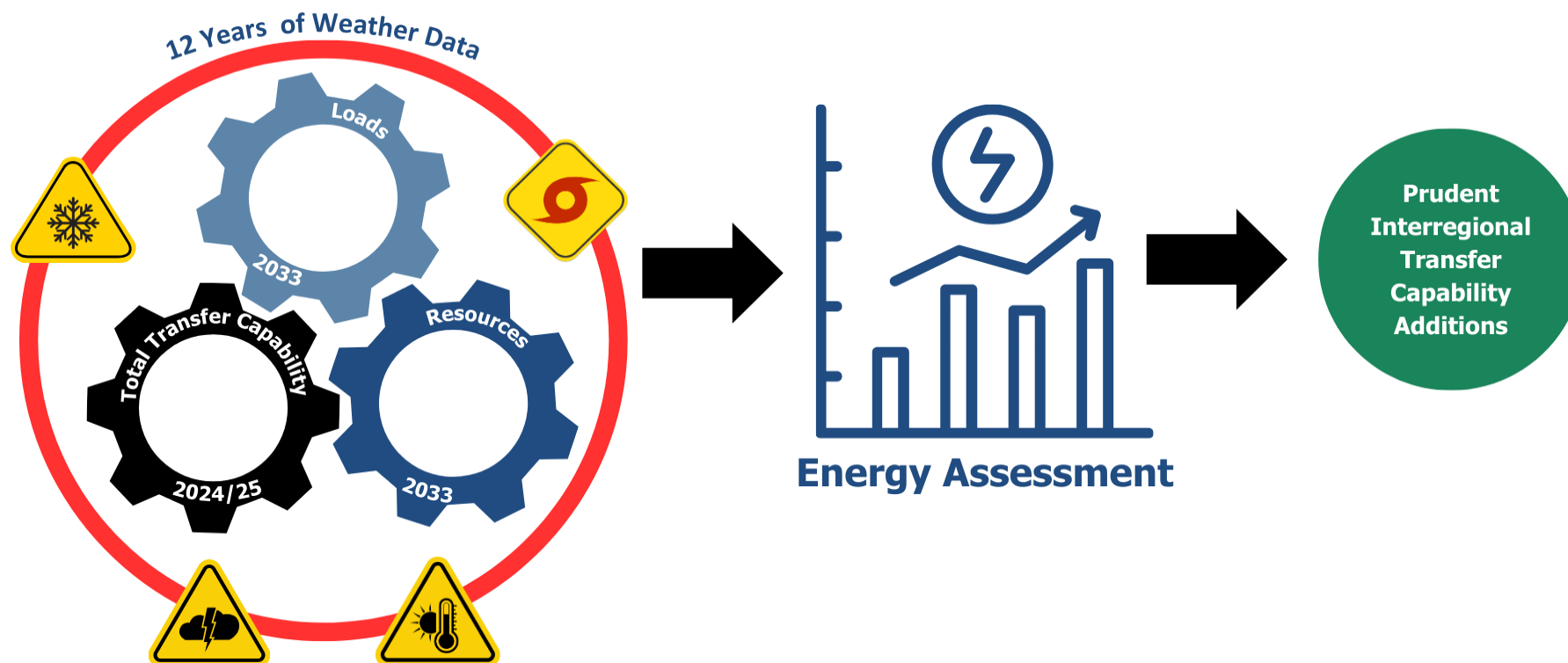


● To be evaluated in Canadian analysis



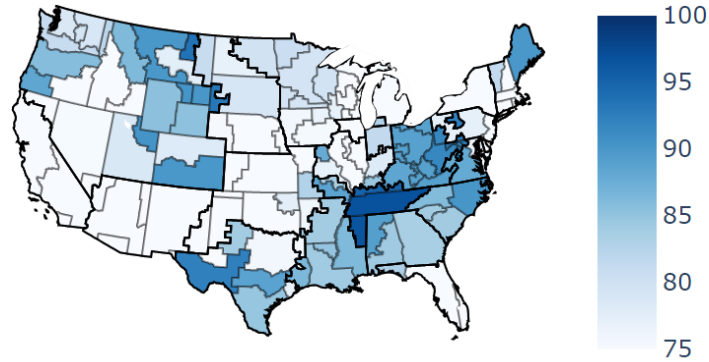


FERC precedent provides that “prudence” means a determination of whether a reasonable entity would have made the same decision in good faith under the same circumstances, and at the relevant point in time.

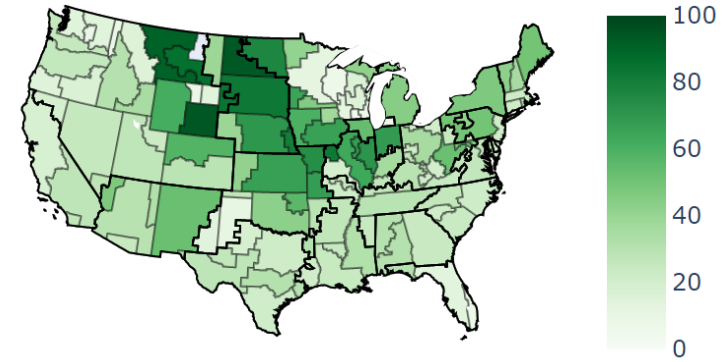


Energy Assessment: Cold Snap Example

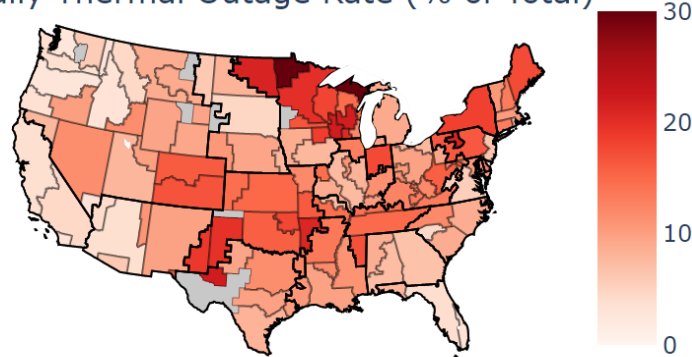
Maximum Daily Load (% of Annual Peak)



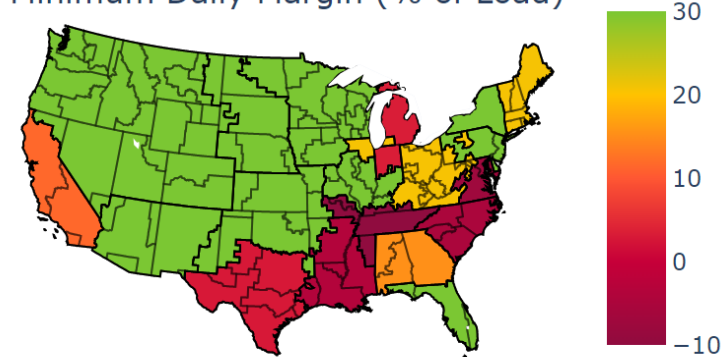
Average Daily Wind & Solar Capacity Factor (%)



Daily Thermal Outage Rate (% of Total)

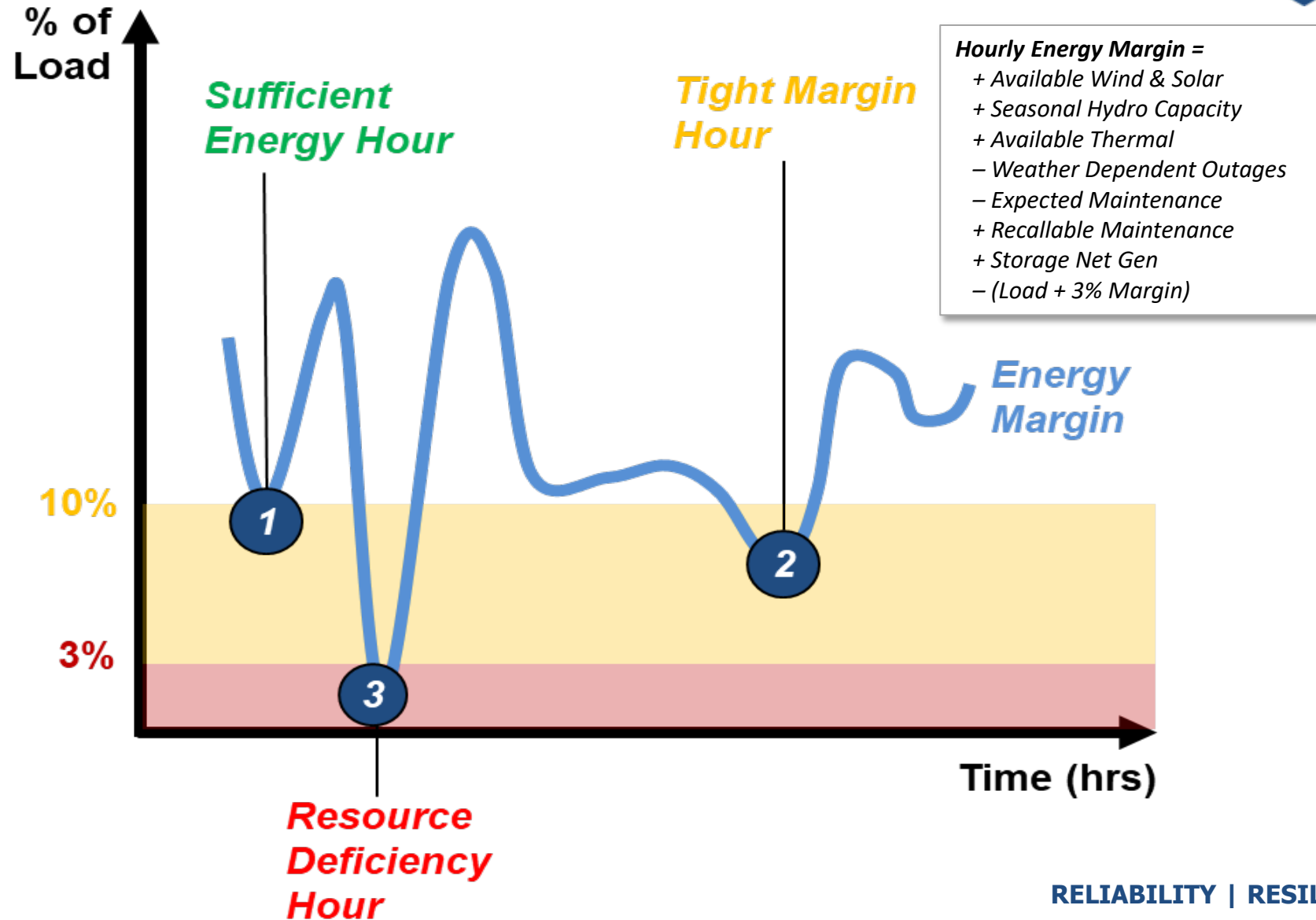


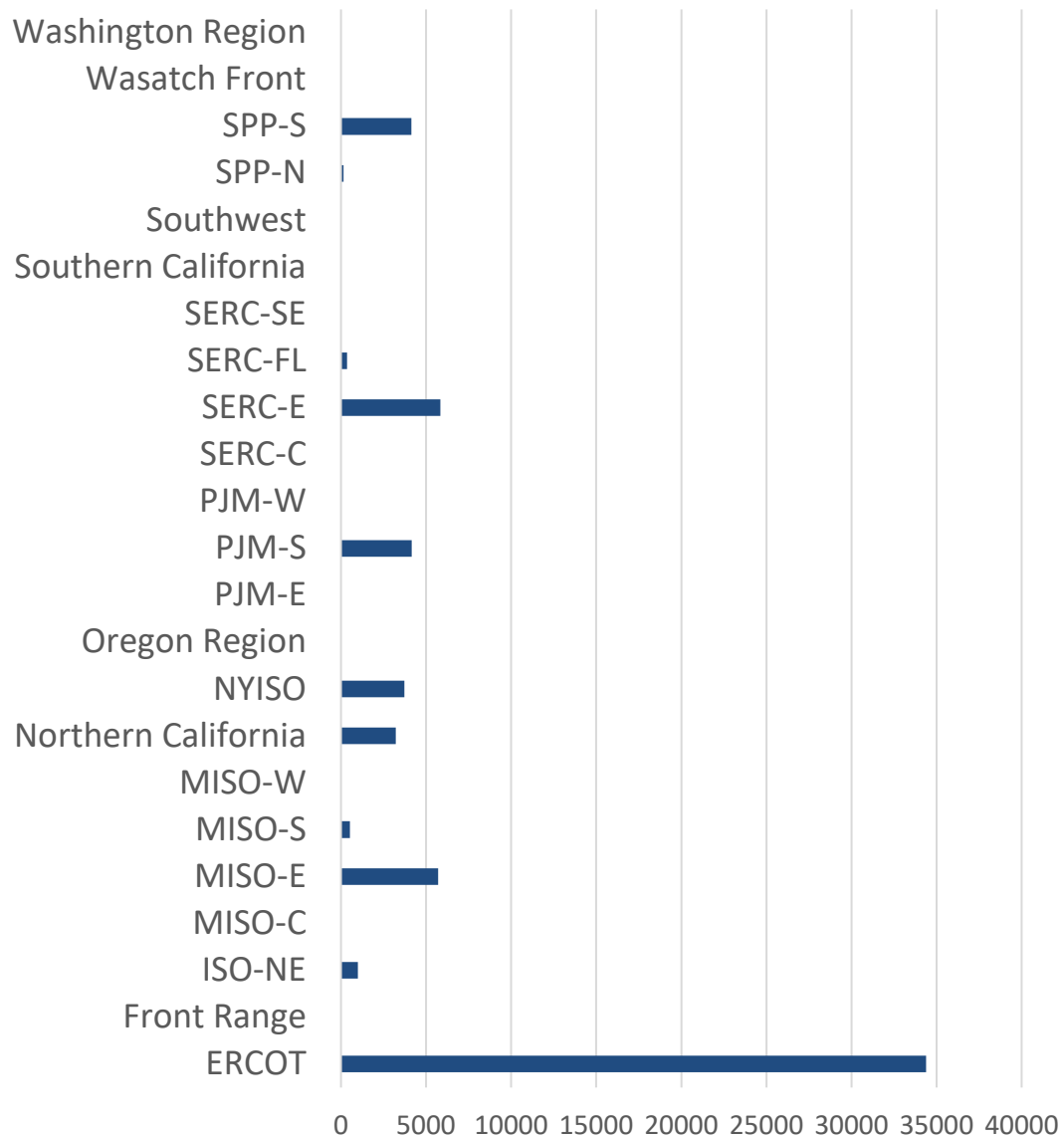
Minimum Daily Margin (% of Load)



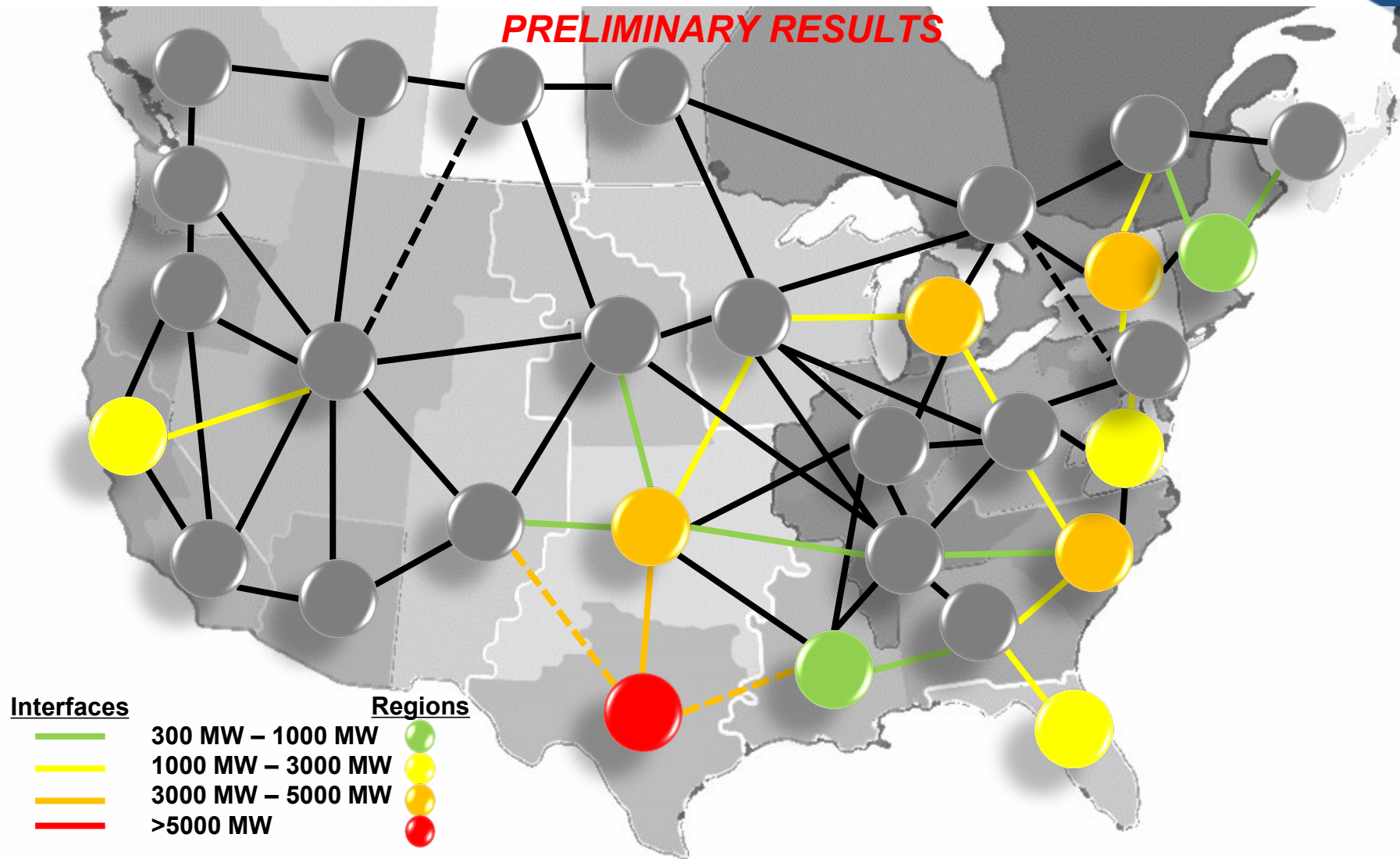
Source: ESIG Transmission Resilience Task Force (Telos Energy)
<https://www.esig.energy/transmission-resilience/>

Energy Assessment to Identify Prudent Additions



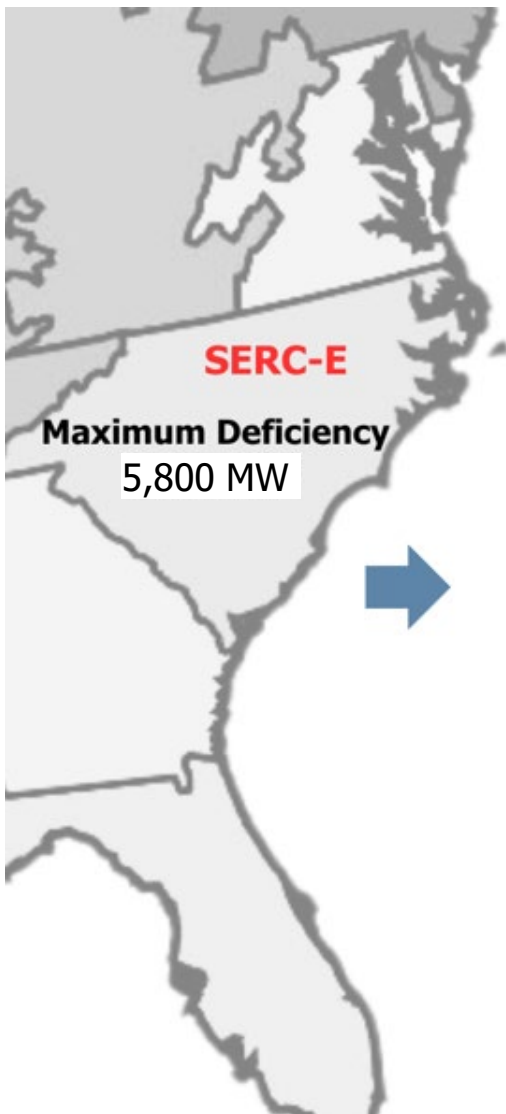


- Capacity expansion determined by projections in Long-Term Reliability Assessment
- Tightening energy margins driven:
 - assumed extreme weather conditions
 - increased load growth
 - on-going retirement of conventional generation
 - shift toward a higher proportion of variable (wind and solar)
 - energy-limited resources (e.g., battery storage).
- Number of hours in these conditions range from 1-20

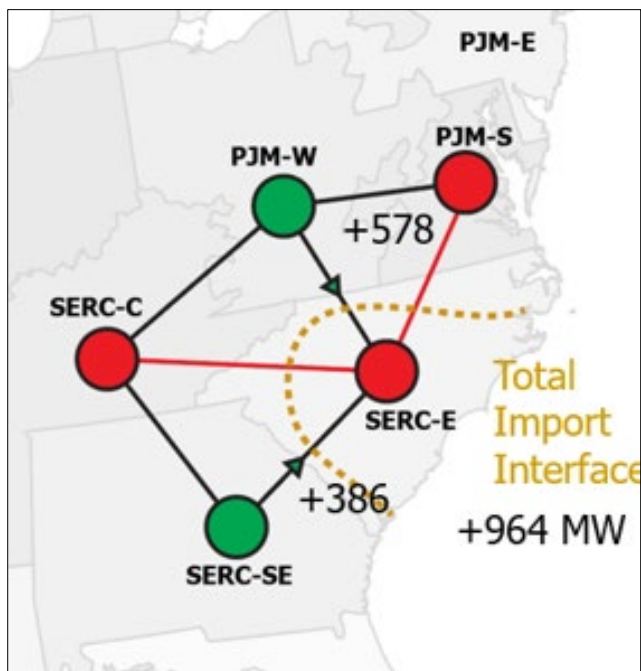


Recommended Prudent Additions (Preliminary)

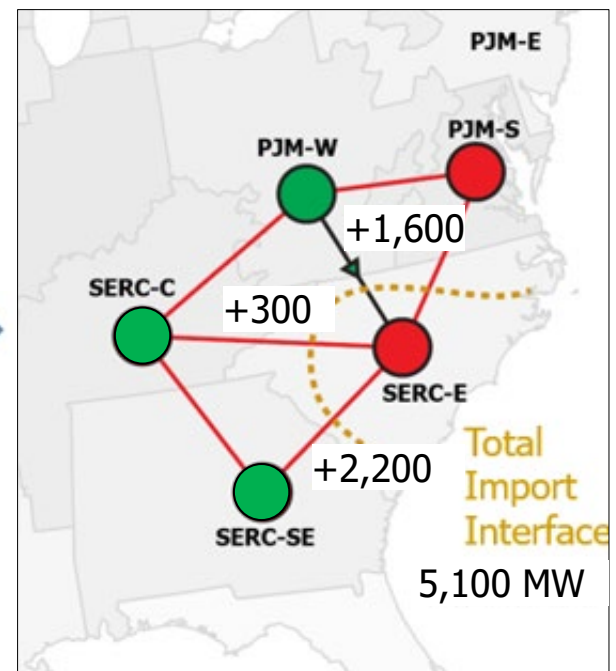
Recommended Prudent Additions				
Transmission Planning Region	Events / Drivers	Event Seasons	Interface for Additions	Prudent Addition Recommendation (MW)
Northern California	2022 Heat Wave	Summer	Wasatch Front	1,100
ERCOT	Winter Storm Uri (2021) and four other events	Summer and Winter	Front Range, MISO-S, SPP-S	14,100
SPP-S	Winter Storm Uri (2021)	Winter	ERCOT, Front Range, MISO-W, SERC-C, SPP-N	4,200
MISO-E	2020 and two other events	Summer	MISO-W, PJM-W	3,000
MISO-S	2009 and 2011	Summer	ERCOT, SERC-SE	600
SERC-FL	2021 and two other events	Summer and Winter	SERC-SE	1,400
SERC-E	Winter Storm Elliott (2022)	Winter	PJM-W, SERC-C, SERC-SE	4,100
PJM-S	Winter Storm Elliott (2022)	Winter	PJM-E	2,800
NYISO	2023 Heat Wave and five other events	Summer	PJM-E, Québec	3,100
ISONE	2012 and two other events	Summer	Québec, Maritimes	700
Total Prudent Additions Recommendations				35,100



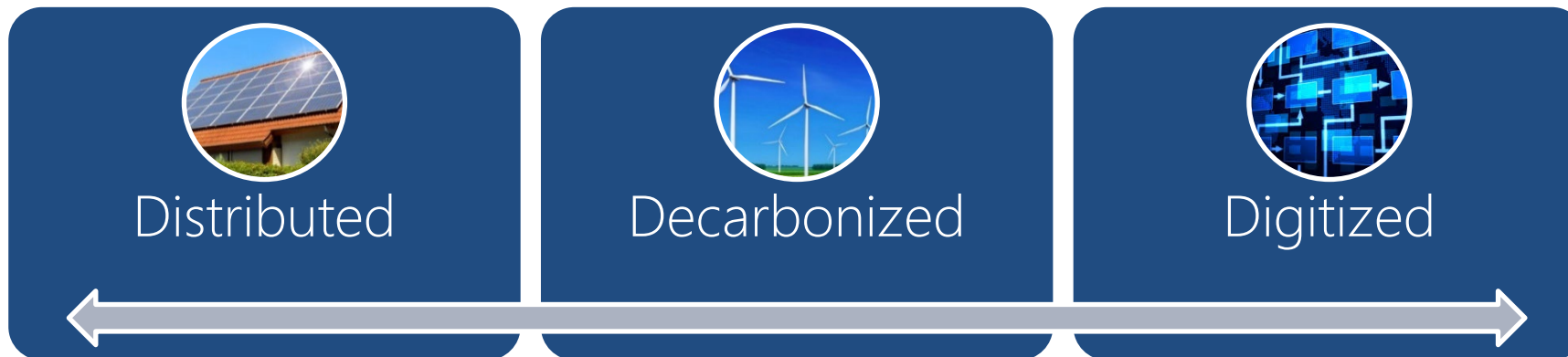
First Iteration: Utilize Existing Import Capability and Excess Available Generation from Neighbors



Third Iteration: Maximum Support from Neighbors, Prioritized by Excess Available Generation



1,000 MW of Existing Import Capability + 4,100 MW of Prudent Additions = **5,100 MW of Needed Import Capability** from PJM-W, SERC-C, and SERC-SE



Must Wins:

1. **Build more capacity and manage the pace of transformation** through market mechanisms and inter-agency coordination on policies that impact generation.
2. Ensure a robust **energy supply chain** for the balancing resources, with sufficient access to fuel and stored energy to withstand long-duration, wide-spread extreme weather events
3. Develop sufficient **transmission**, to integrate renewables and distribute them, make the system more resilient
4. Maintain a robust fleet of **balancing resources**, with an ability to provide **Essential Reliability Services** to ensure inverter-based resources don't negatively impact reliability
5. **STATES:** Refine resource adequacy requirements that preserves energy assurance



Questions and Answers

HOW TO DEVELOP A RESPONSIVE WORKFORCE TO ADDRESS THE THREATS OF THE FUTURE

TIM CONWAY

Technical Director, ICS at SANS
Institute



SANS

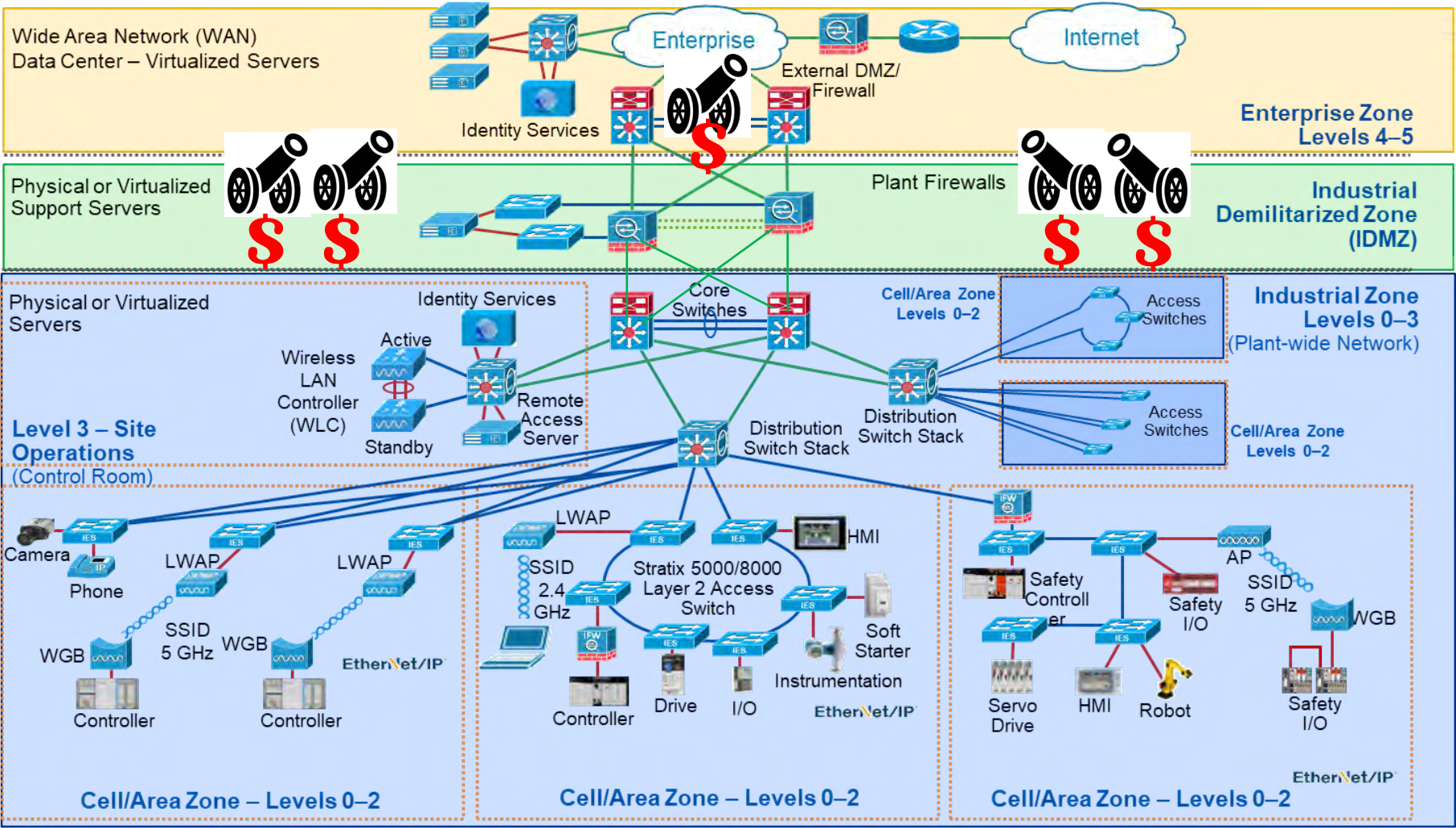
How to Develop a Responsive Workforce to Address the Threats of the Future

AKA: Workforce for Today and Tomorrow

Tim Conway

- SANS Institute ICS Curriculum
 - Senior Instructor
 - Course Author
-

Threats of the Future?



Offensive Progressions

Critical Infrastructure targeting

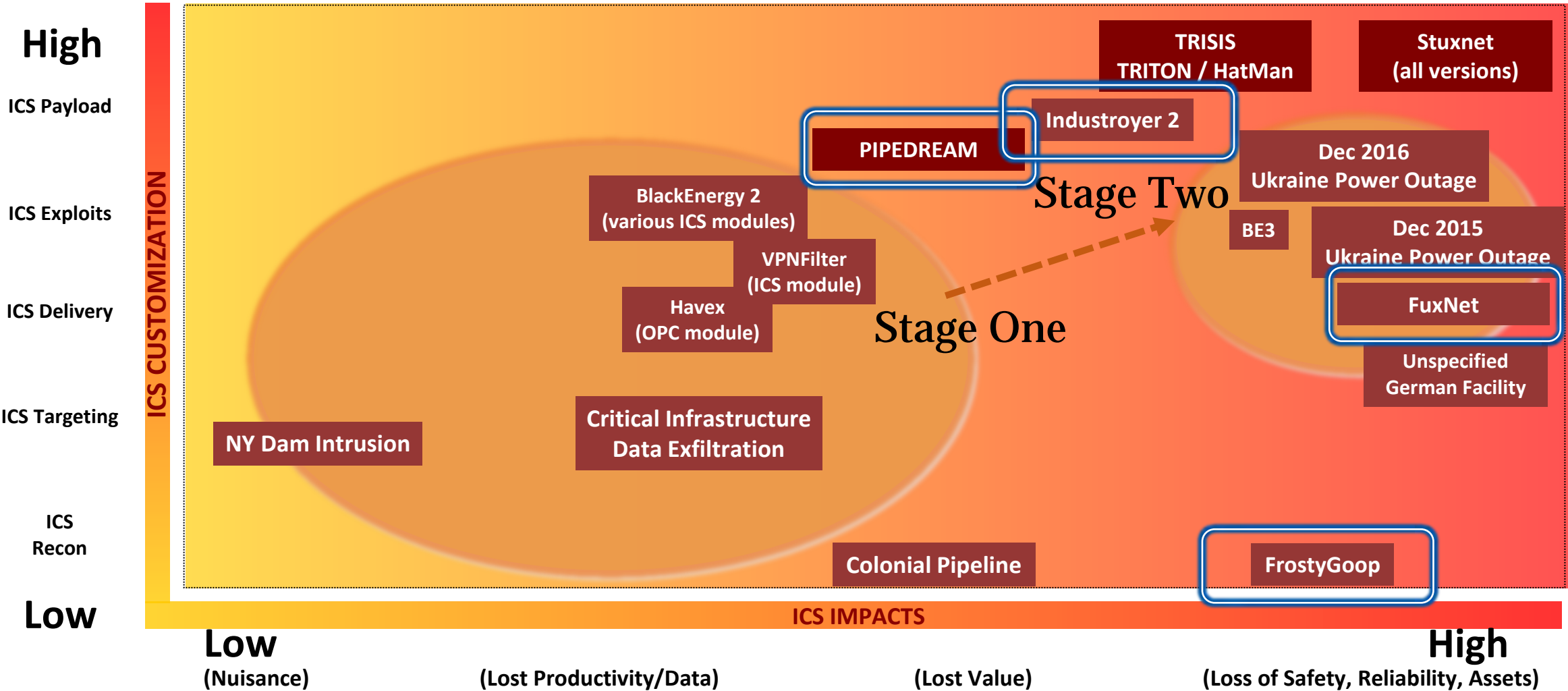
Progression in All Categories



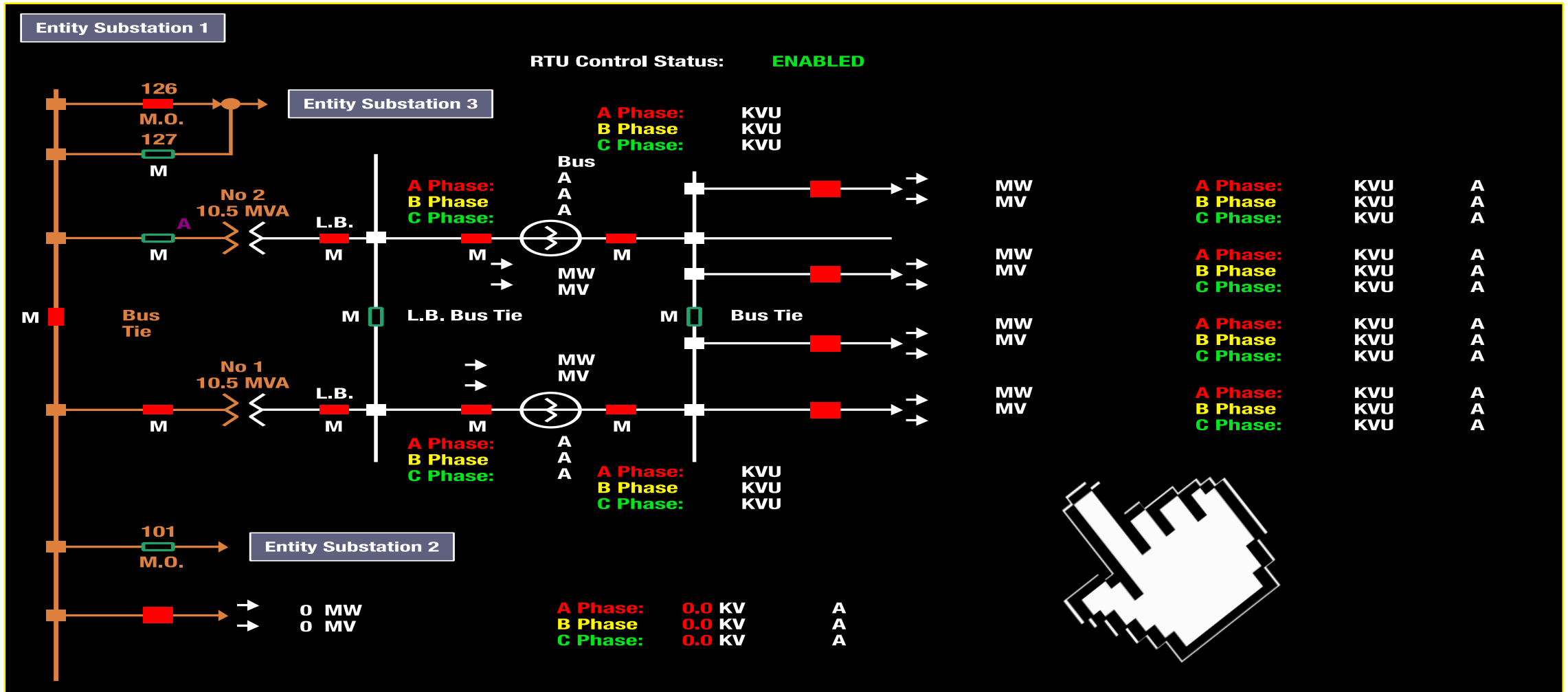
Governance,
Standards,
Regulation,
Architecture,
Cyber Hygiene,
Passive Defense

Operations
Resilience,
Cyber Engineering,
Active Defense

ICS Incidents & Access Campaigns



Electric System Cyber Attacks



Malware Discovery Associated with Electric Outages

Russia has developed a cyberweapon that can disrupt power grids, according to new research



The malware, dubbed CrashOverride, is just the second instance of malware specifically tailored to disrupt or destroy industrial control systems, according to new research. The Washington Post's Ellen Nakashima explains. (The Washington Post)

By Ellen Nakashima June 12 at 4:20 PM

Hackers allied with the Russian government have devised a cyberweapon that has the potential to be the most disruptive yet against electric systems that Americans depend on for daily life, according to U.S. researchers.

ANDY GREENBERG SECURITY 06.19.17 12:41 PM

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID

Cyber firms warn of malware that could cause power outages

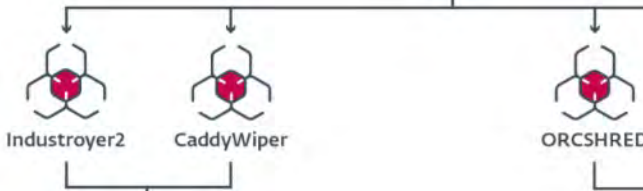


Two in a Month – Anticipate Many More



Sandworm

Deploy

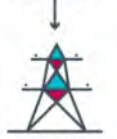


ICS network

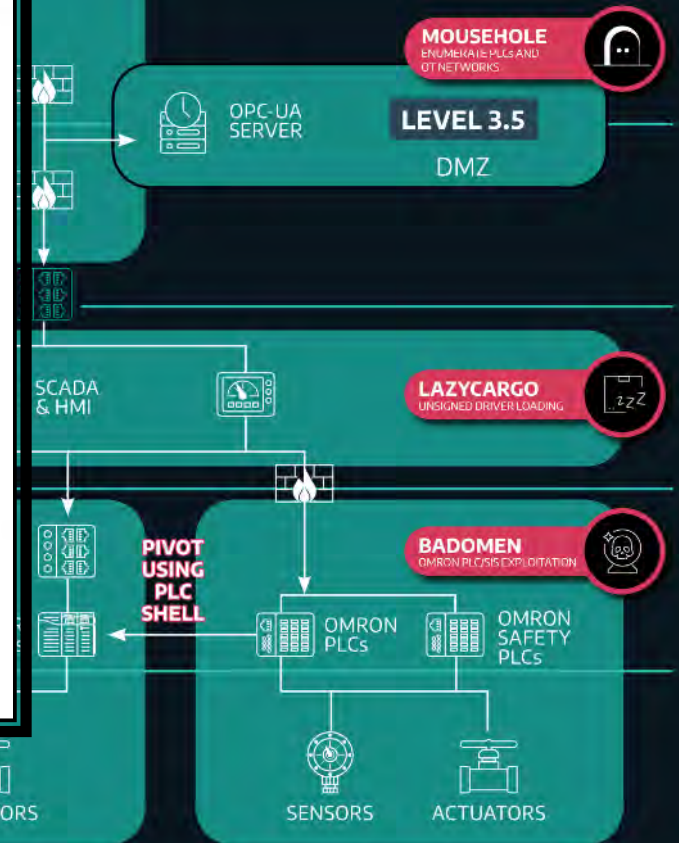


- 4/8/2022 15:02:22 scheduled task to launch Industroyer2
- 4/8/2022 16:10 scheduled execution of industroyer2
- 4/8/2022 16:20 scheduled execution of CaddyWiper
- Industroyer2 only implements IEC-104
- Industroyer2 is recompiled for each victim environment

Control



Electrical substation



PIPEDREAM

Past, Present, and Future



- Ongoing coordinated cyber & physical attacks
- Critical Infrastructure impacts enabling invasion and entrenchment



- Positioning, capability validation, effects-based attacks
- Targeted service outages and equipment damaging attacks

Coordinated Cyber & Physical Attacks

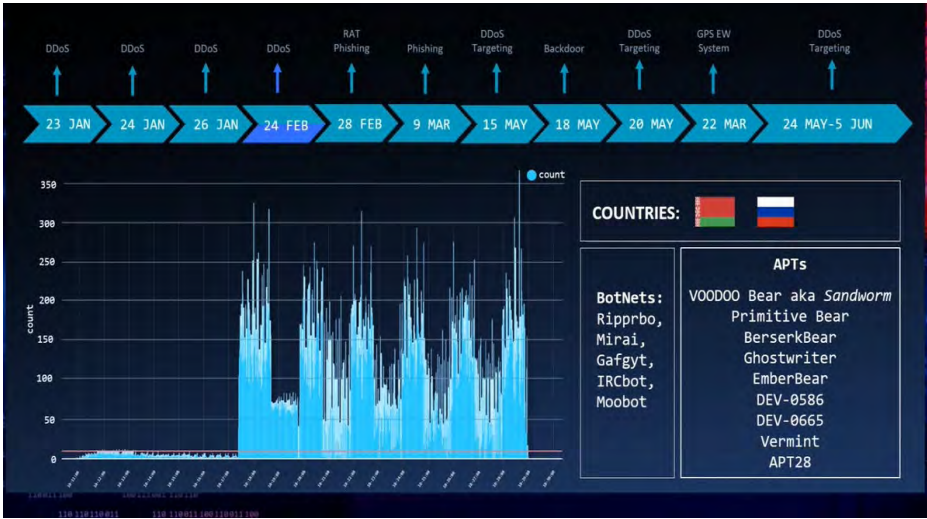


ATTRACTED

372 000 000 €

of credit and grant funds from the EBRD and the government of the Netherlands

- to restore the networks after russian missile attacks
- to improve the Company's financial stability



Defensive Progression Needed

Experts at operating complexity, need to consider misuse

What Would You Say You Do Here?

Leaders

Step up
Step over
Build and Manage a Team
Pursue executive support
Enable the team

+ **Compliance**

+ **Cybersecurity**

Operators

Know the system
Know the tools
Normal / Conservative / Emergency Op
Restoration and response with technology impacts

+ **Compliance**

+ **Cybersecurity**

+ **Compliance**

+ **Cybersecurity**

Physical Security

Physical security monitor and defense
Site Assessment and remediation
Security incident response
Information sharing and ingest

+ **Compliance**

+ **Cybersecurity**

IT / OT

System / Network / Application build / support
Operational ICS System design / build / support
Cybersecurity defense / detection / response
Recovery / restoration
Information sharing and ingest

Safety First, Injuries Last

Regardless of Job title – everyone plays a role in cybersecurity and Compliance



Building a Cyber Skilled Workforce For Today and Tomorrow

Security Team Axioms

If you're lucky...

- you'll inherit a good team
- you'll get to choose your team
- you'll be able to build a good team

If you're good...

- you'll get to stick around
- your team may stick around
- Others will want to join your team

If your team is good...

- people will want to steal your team



Find, Attract, & Retain

Do they
exist

Can you
hire
them

Will you
keep
them

What Capability Levels & How Many at a Given Level

ICS CYBERSECURITY SKILLSETS AND ROLES

ICS Knowledge Levels

As an ICS team's skillsets and roles are considered, the ICS Knowledge Levels can be used to guide the development plans for team members, tasks, roles, and responsibilities. Each knowledge level can be used to build a strong ICS security team and establish and mature an ICS security program.



Base Knowledge – LEVEL 0

Base knowledge training should focus on security behaviors for individuals who interact with, operate, or support industrial control systems. A training program may introduce ICSs, the risks or types of ICS attacks, basic system and network defenses and controls, as well as typical ICS governance and policy best practices. The training program's goal should be to change human behavior in an ICS environment and reduce risk at a fundamental level.



Foundational Knowledge – LEVEL 1

Foundational knowledge training should ensure the workforce involved in supporting and defending industrial control systems are trained to keep the operational environment safe, secure, and resilient against current and emerging ICS cyber threats. Across a diverse audience, this training level should build, develop, and ensure a common language in control systems and an understanding of the underlying engineering processes while providing an overview of the basic tools specific to ICS security across a wide range of industry sectors and applications.



Mastery Knowledge – LEVEL 2

Mastery knowledge training should be role-specific and focus on individuals and organizational needs to advance ICS cybersecurity defense knowledge, skills, and ability in a specific field, architect proper ICS network architecture, and conduct incident response and recovery practices with engineering teams.



Expert Knowledge – LEVEL 3

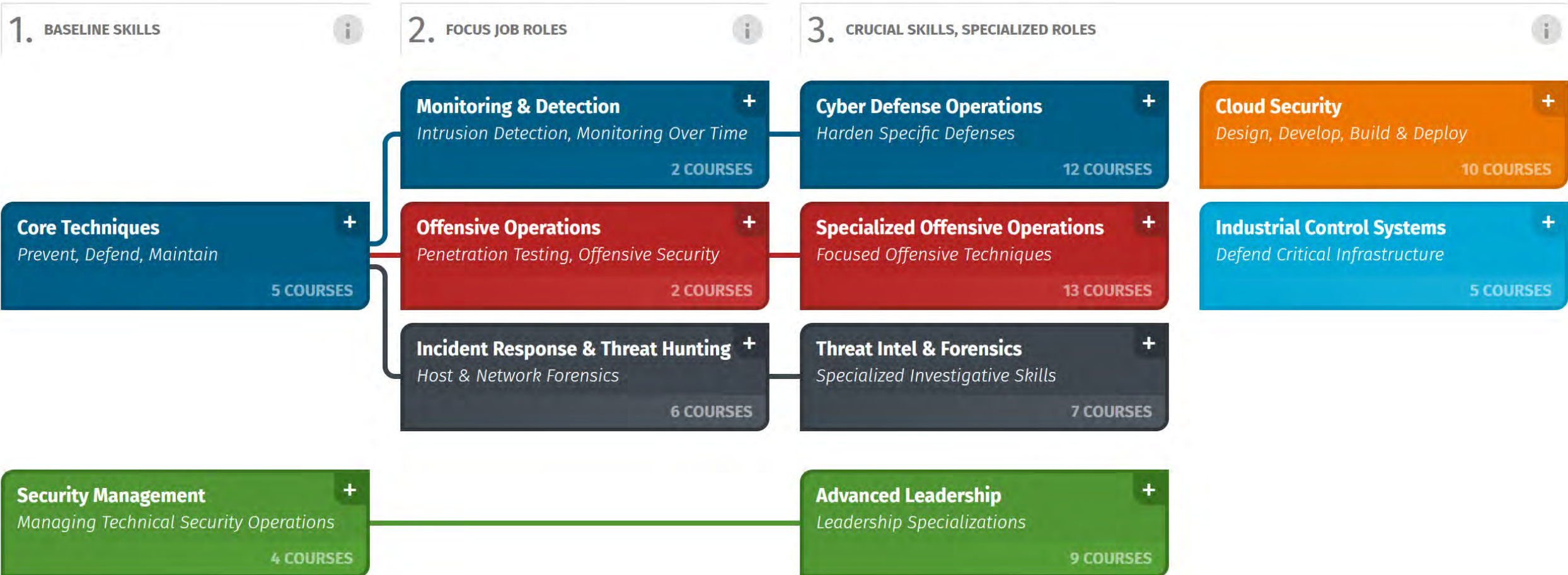
Expert knowledge training should focus on coordinated industrial advanced incident response and improving team capabilities and toolsets. Expert training typically consists of joint exercises and projects with engineering and other facility teams.



Leader – LEVEL 4

ICS cybersecurity leadership training should focus on technical team development and leadership, risk management, approaches for building relationships with other teams, tracking meaningful metrics, maturing the overall ICS cybersecurity program, and communicating technical concepts to non-technical audiences, including reporting to the board.

One Provider – Cybersecurity Focused 75 Courses



IT – Information Technology and OT Operational Technology



Data at rest, data in motion, and
data in use



Data that does something in the
physical world – kinetic component

COOLEST CAREERS IN CYBER

Organizations are hiring individuals with a unique set of skills and capabilities, and seek those who have the abilities and knowledge to fulfill many new job roles in the cybersecurity industry. The coolest careers in cybersecurity are the most in demand by employers. Which jobs are the coolest and most in demand? We know, so let us show you the hottest cybersecurity jobs for 2024.

Curricula: NewCyber Cyber Defense Digital Forensics Offensive Operations Cybersecurity Leadership Cloud Security Industrial Control Systems Purple Team SEC400 GDM ← GIAC Certification with course

01 Threat Hunter (Threat/Warning Analyst)

This expert applies new threat intelligence against existing evidence to identify attackers that has slipped through real-time detection mechanisms. The practice of threat hunting requires several skill sets, including threat intelligence, system and network forensics, and investigation development processes. This role transitions incident response from a purely reactive investigative process to a proactive one, uncovering adversaries or their footprints based on developing intelligence.

Why is this role important?
Threat hunters proactively seek evidence of attackers that were not identified by traditional detection mechanisms. Their discoveries often include latent adversaries that have been present for extended periods of time.

Recommended courses
FOR508 GDM FOR332 FOR572 GDM FOR578 GDM FOR608 FOR101 GDM
SEC497 GDM SEC504 GDM SEC505 GDM ICS516 GDM

"Digging below what others see after this threat is hidden from threat actors in a client environment. This is no special. Shoutout to SANS and Threat Intelligence Analysts who continue to push the boundaries of what's possible in the field."
-Ali Mubarek

02 Red Teamer (Adversary Emulation Specialist)

In this role you will be challenged to look at behaviors and situations from the perspective of an adversary. The focus is on making the blue team better by testing and measuring the organization's detection and response policies, procedures, and technologies. This role includes performing adversary emulation, a type of red team exercise where the red team emulates how a threat actor would behave, following the same tactics, techniques, and procedures (TTPs), with a specific objective similar to those of realistic threats or adversaries. It can also include creating custom implants and C2 frameworks to evade detection.

Why is this role important?
This role is important to help assess the common question of "can that attack that brought down company, happen to us?" Red Teamers will have a holistic view of the organization's preparedness for a real, sophisticated attack by testing the defenders, not just the defenses.

Recommended courses
SEC208 GDM SEC542 GDM SEC560 GDM SEC565 GDM
SEC660 GDM SEC670 SEC699 SEC740

"The only way to test a Red Teamer is to have a full catalog of offensive security tools, frameworks, Security Operations and having the best offensive and defensive operations from various vendors and to be able to integrate them into a single environment where it can be used for testing."
-Reuben Cho

03 Digital Forensic (Cyber Defense Forensics Analyst)

This expert applies digital forensic skills to a plethora of media that encompasses an investigation. The practice of being a digital forensic examiner requires several skill sets, including evidence collection, computer, smartphone, cloud, and network forensics, and an investigative mindset. These experts analyze compromised systems or digital media involved in an investigation that can be used to determine what really happened. Digital media contain insights that physical forensic data and the crime scene may not include.

Why is this role important?
You are the sleuth in the world of cybersecurity, searching computers, smartphones, cloud data, and networks for evidence in the wake of an incident/crime. The opportunity to learn never stops. Technology is always advancing, as is your career.

Recommended courses
FOR308 FOR498 GDM FOR500 GDM FOR508 GDM FOR509 GDM FOR181 GDM
FOR387 FOR572 GDM FOR585 GDM SEC401 GDM SEC401 GDM

"Forensics is about taking deep dives into systems and devices to find out what happened. It's a mix of technical and investigative skills to develop a solution."
-Patrick M

"This isn't just IT, and the technical forensics, but it's also about the human side of things. You're not just a technician, you're a detective."
-Anthony Wu

04 Purple Teamer

In this fairly recent job position, you have a keen understanding of both how cybersecurity defenses ("blue team") work and how adversaries operate ("red team"). During your day-to-day activities, you will organize and automate emulation of adversary techniques, highlight possible new log sources and use cases that help increase the detection coverage of the SOC, and propose security controls to improve resilience against the techniques. You will also seek to help coordinate effective communication between traditional defensive and offensive roles.

Why is this role important?
Help blue and red understand one another better. Blue teams have traditionally been talking about security controls, log sources, use cases, etc. On the other side, red teams traditionally talk about payloads, exploits, implants, etc. Help bridge the gap by ensuring red and blue are speaking a common language and can work together to improve the overall cybersecurity posture of the organization.

Recommended courses
SEC599 GDM SEC690 SEC504 GDM SEC568 SEC598

"The combination of red team and blue team work is what you get to see both sides. I have been a Purple Teamer for a while now and it has changed a lot of positive change for us."
-Anissa A

05 Malware Analyst

Malware analysts investigate and analyze malicious software to understand how it works, how it spreads, and what it has done, in order to prevent future incidents.

Why is this role important?
If you're good at understanding the behavior of malicious code, you know you're in a great position to investigate and analyze malware. This role requires a deep understanding of how malware works, how it spreads, and what it has done, in order to prevent future incidents.

Recommended courses
FOR518 GDM FOR519 GDM FOR520 GDM FOR521 GDM FOR522 GDM FOR523 GDM

"Being a malware analyst provides a great opportunity to get your hands dirty with the most complex and dangerous of malware. It's a role that gives you the power to make the difference between a victim and a victor."
-Rob Ferrell

06 Chief Information Security Officer (CISO) (Executive Cyber Leadership)

The CISO leads staff in identifying, developing, implementing, and maintaining processes across the organization to reduce information and information technology risks. CISOs respond to incidents, establish appropriate standards and controls, manage security technologies, and direct the establishment and implementation of policies and procedures. The CISO is also centrally responsible for information-related compliance, such as supervising efforts to achieve ISO/IEC 27001 certification for an entity or a part of it. Typically, the CISO's influence reaches the entire organization.

Why is this role important?
The need for CISOs has grown as a result of business, academic, and technology knowledge in order to be up to speed on information security issues from a technical standpoint, understand how to implement security planning into the broader business objectives, and be able to build a longer lasting security and risk based culture to protect the organization.

Recommended courses
LDR512 GDM LDR514 GDM LDR515 LDR520 LDR521 LDR521 GDM LDR533
SEC360 GDM ICS410

"The chief info security officer is the person who has the most responsibility to ensure the security of the organization. They are the ones who are responsible for the security of the organization and the people who work for them."
-Amelion Edwards

07 Blue Teamer - All-Around Defender (Cyber Defense Analyst)

This job, which may have varying titles depending on the organization, is often characterized by the breadth of tasks and knowledge required. The all-around defender and blue teamer is the person who may be a primary contact for a small organization, and must deal with engineering and architecture, incident triage and response, security tool administration and more.

Why is this role important?
This job role is highly important as it often shows up in small to mid-size organizations that do not have budgets for a full-fledged security team with dedicated roles for each function. The all-around defender isn't necessarily an ideal role as it is the scope of the defense work such defenders may do - a little bit of everything for everyone.

Recommended courses
SEC400 SEC503 GDM SEC505 GDM SEC511 GDM
SEC530 GDM SEC535 GDM SEC586

"In this day and age, you need to be a jack of all trades and a master of many. You need to be able to defend and protect the network from all angles."
-Drew C

08 Security Architect (NICE) and Engineer

Design, implement, and tune an effective combination of network-centric and data-centric controls to balance prevention, detection, and response. Security architects and engineers are capable of looking at an enterprise defense holistically and building security at every layer. They can balance business and technical requirements along with various security policies and procedures to implement defensible security architectures.

Why is this role important?
A security architect and engineer is a versatile blue teamer and cyber defender who possesses an arsenal of skills to protect an organization's critical data, from the endpoint to the cloud, across networks and applications.

Recommended courses
SEC503 GDM SEC505 GDM SEC511 GDM SEC530 GDM SEC549

"A security architect needs to be able to understand how networks, networks, networks, business requirements, and how they all fit together. It's a role that requires a deep understanding of the organization's needs and how to protect them."
-Chris Bost

09 Cyber Defense Incident Response Analyst

This dynamic and fast-paced role involves responding to security incidents and conducting investigations to identify the cause of an incident and prevent future occurrences.

Why is this role important?
While preventing breaches is always the goal, it is not always possible. When a breach does occur, it is the responsibility of the incident response analyst to quickly identify the cause of the breach, contain the damage, and prevent further incidents.

Recommended courses
FOR508 GDM FOR509 GDM FOR510 GDM FOR511 GDM FOR512 GDM FOR513 GDM FOR514 GDM FOR515 GDM FOR516 GDM FOR517 GDM FOR518 GDM FOR519 GDM FOR520 GDM FOR521 GDM FOR522 GDM FOR523 GDM

"Incidents are bound to occur and it's important to have a team that can respond quickly and effectively. This role requires a deep understanding of the organization's needs and how to protect them."
-Arieh A

10 Cybersecurity Analyst/Engineer (Systems Security Analyst)

As this is one of the highest paid jobs in the field, the skills required to master the responsibilities involved are advanced. You must be highly competent in threat detection, threat analysis, and threat prevention. This is a vital role in preserving the security and integrity of an organization's data.

Why is this role important?
This is a proactive role, creating contingency plans that the company will implement in case of a successful attack. Since cyber attackers are constantly using new tools and strategies, cybersecurity analysts/engineers must stay informed about the tools and techniques out there to ensure a strong defense.

Recommended courses
SEC401 GDM SEC450 SEC501 GDM SEC502 GDM SEC530 GDM SEC535 GDM SEC599 GDM
SEC504 GDM SEC594 SEC598 GDM FOR509 GDM LDR515 LDR521 GDM LDR533 GDM
SEC340 GDM SEC348 ICS410 GDM ICS456 GDM

"I don't think there's much more valuable than the fact that you can protect your organization's data and assets. It's a role that gives you the power to make the difference between a victim and a victor."
-Jacob Ford

11 OSINT Investigator/Analyst

These researchers professionalize general requirements from their financials and then, using open sources and mostly resources on the internet, collect data relevant to their investigation. They may research domains and IP addresses, businesses, people, issues, financial transactions, and other targets in their work. Their goals are to gather, analyze, and report their objective findings to their clients that the clients might gain insight on a topic or issue prior to acting.

Why is this role important?
This is a massive amount of data that is accessible on the internet. The issue that many people have is that they do not understand how best to discover and harvest this data. OSINT investigators have the skills and resources to discover and obtain data from sources around the world. They support people in other areas of cybersecurity, intelligence, military, and business. They are the finders of things and the knowers of secrets.

Recommended courses
SEC497 GDM SEC587 FOR578 GDM

"Being an OSINT analyst is a role that requires a deep understanding of the organization's needs and how to protect them. It's a role that gives you the power to make the difference between a victim and a victor."
-Anissa A

12 Technical Director (Information Systems Security Manager)

This expert defines the technological strategies in conjunction with development teams, assesses risk, establishes standards and procedures to measure progress, and participates in the creation and development of a strong team.

Why is this role important?
With a wide range of technologies in use that require more time and knowledge to manage, a global shortage of cybersecurity talent, an unprecedented migration to cloud, and a legal and regulatory compliance often increasing and complicating the matter more, a technical director plays a key role in successful operations of an organization.

Recommended courses
LDR512 GDM LDR514 GDM LDR515 LDR520 GDM LDR521 GDM LDR533 GDM ICS410

"A technical director must have strong cybersecurity knowledge and a deep understanding of the organization's needs and how to protect them. It's a role that requires a deep understanding of the organization's needs and how to protect them."
-Francisco Lopez

13 Cloud Security Analyst

The cloud security analyst is responsible for cloud security architecture, configuration, and testing of tools for configuration management, assessing the overall cloud security posture, and providing technical expertise for organizational decision-making.

Why is this role important?
With an unprecedented move from traditional on-premise to cloud, the need for cloud security experts is growing. This position helps secure a company's data and applications in a multi-cloud environment.

Recommended courses
SEC408 GDM SEC510 GDM SEC541 GDM SEC401 GDM
FOR509 GDM SEC588 GDM

"This role is essential to ensure that your organization's data and applications are secure in the cloud. It's a role that gives you the power to make the difference between a victim and a victor."
-Josh W

14 Intrusion Detection/SOC Analyst (Cyber Defense Analyst)

Security Operations Center (SOC) analysts work alongside security engineers and SOC managers to implement prevention, detection, monitoring, and action response. Working closely with incident response teams, a SOC analyst will address security issues when detected, quickly and effectively. With an eye for detail and anomalies, these analysts see things most others miss.

Why is this role important?
SOC analysts help organizations have greater speed in identifying attacks and remediating them before they cause more damage. They also help meet regulatory requirements that require security monitoring, vulnerability management, or an incident response function.

Recommended courses
SEC430 SEC503 GDM SEC511 GDM SEC535 GDM
FOR508 GDM FOR572 GDM FOR572 GDM SEC504 GDM

"The intrusion analyst is the person who is responsible for detecting and stopping intrusions. They are the ones who are responsible for the security of the organization and the people who work for them."
-Chuck Bost

15 Security Awareness Officer (Security Awareness & Communications Manager)

Security Awareness Officers work alongside their security team to identify their organization's top human risks and the behaviors that manage those risks. They are then responsible for developing and managing a continuous program to effectively train and communicate with the workforce to exhibit those secure behaviors. Highly mature programs not only impact workforce behavior but also create a strong security culture.

Why is this role important?
People have become the top drivers of incidents and breaches today, and yet the problem is that most organizations still approach security from a purely technical perspective. Your role will be key in making your organization to realize that gap and address the human side also. Arguably one of the most important and fastest growing fields in cyber security today.

Recommended courses
LDR533 GDM LDR572 GDM ICS410

"This role allows me to help my organization improve its security awareness. It's a role that gives you the power to make the difference between a victim and a victor."
-Drew C

16 Vulnerability Researcher & Exploit Developer (Vulnerability Assessment Analyst)

In this role, you will work to find 0-days (unknown vulnerabilities) in a wide range of applications and devices used by organizations and consumers. Find vulnerabilities before the adversary.

Why is this role important?
Researchers are constantly finding vulnerabilities in popular products and applications ranging from internet of things (IoT) devices to commercial applications and network devices. Once medical devices, such as insulin pumps and pacemakers, are targets, if we don't have the expertise to research and find these types of vulnerabilities before the adversaries, the consequences can be grave.

Recommended courses
SEC660 GDM SEC670 SEC760

"I think researchers will play a crucial role in the future. There is an increasing number of vulnerabilities being discovered and it's important to have people who can find and exploit them. It's a role that gives you the power to make the difference between a victim and a victor."
-Anissa A

17 Application Pen Tester (Secure Software Assessor)

Application penetration testers probe the security integrity of a company's applications and defenses by evaluating the attack surface of all in-scope vulnerable web-based services, client-side applications, servers-side processes, and more. Mimicking a malicious attacker, app pen testers work to bypass security barriers in order to gain access to sensitive information or enter a company's internal systems through techniques such as pivoting or lateral movement.

Why is this role important?
Web applications are critical for conducting business operations, both internally and externally. These applications often use open source plugins which can put these apps at risk of a security breach.

Recommended courses
SEC542 GDM SEC560 GDM SEC575 GDM SEC588 GDM
SEC660 GDM SEC760

"It's not only about finding vulnerabilities, it's about understanding the logic of the application and how it works. It's a role that gives you the power to make the difference between a victim and a victor."
-Drew C

18 ICS/OT Security Assessment Consultant (ICS/SCADA Security Engineer)

One foot in the exciting world of offensive operations and the other foot in the critical process control environments essential to life. Discover system vulnerabilities and work with asset owners and operators to mitigate discovered and prevent exploitation from adversaries.

Why is this role important?
Security incidents, both intentional and accidental in nature, that affect OT (primarily in ICS systems) can be considered to be high impact but low frequency (HI/FL), they don't happen often, but when they do the cost to the business can be considerable.

Recommended courses
ICS410 GDM ICS456 GDM ICS515 GDM ICS612 SEC560 GDM

"Working in this type of environment is a great experience. It's a role that gives you the power to make the difference between a victim and a victor."
-Allan Wright

19 DevSecOps Engineer (Information Systems Security Developer)

As a DevSecOps engineer, you develop automated security capabilities leveraging best of breed tools and processes to inject security into the DevOps pipeline. This includes leadership in key DevSecOps areas such as vulnerability management, monitoring and logging, security operations, security testing, and application security.

Why is this role important?
DevSecOps is a natural and necessary response to the bottleneck effect of older security models, or the modern continuous delivery pipeline. The goal is to bridge traditional gaps between IT and security by ensuring fast, safe delivery of applications and business functionality.

Recommended courses
SEC408 GDM SEC570 GDM SEC572 GDM SEC540 GDM

"From my point of view, it's a role that gives you the power to make the difference between a victim and a victor. It's a role that gives you the power to make the difference between a victim and a victor."
-Anissa A

20 Media Exploitation Analyst (Cyber Crime Investigator)

This expert applies digital forensic skills to a plethora of media that encompasses an investigation. If investigating computer crime or data, you will want to make a career of recovering the evidence that has been lost, damaged or used in a crime. This may be the path for you in this position, you will assist in the forensic examinations of computers and media from a variety of sources, in view of developing forensically sound evidence.

Why is this role important?
You are often the first responder or the first to touch the evidence involved in a criminal act. Common cases involve terrorism, counter-intelligence, law enforcement and insider threat. You are the person relied upon to conduct media exploitation from acquisition to final report and are an integral part of the investigation.

Recommended courses
FOR320 FOR498 GDM FOR500 GDM FOR508 GDM FOR181 GDM FOR532
FOR572 GDM FOR585 GDM

"This is the coolest job in the world. It's a role that gives you the power to make the difference between a victim and a victor. It's a role that gives you the power to make the difference between a victim and a victor."
-Chris Bost

Blending Skill Sets

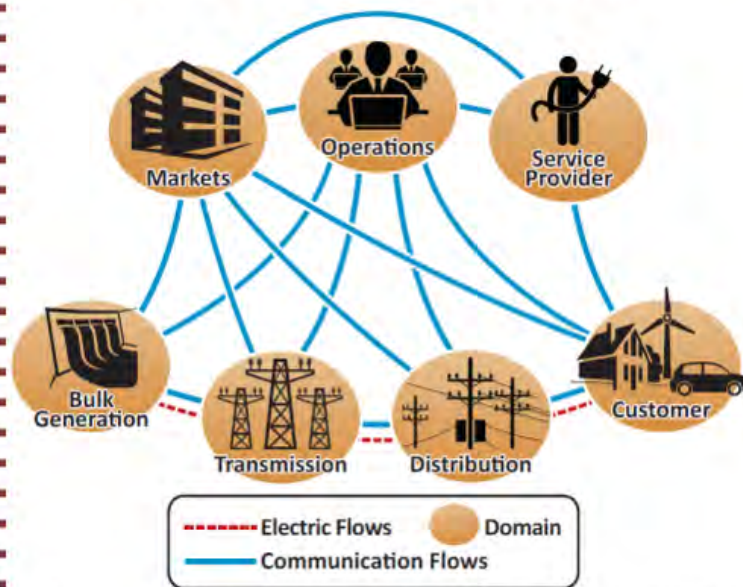
Secure Power System Professionals



Hybrid Skillset



Diverse Work Environment



Based on NIST Smart Grid Framework 1.0, September 2009



#1 Area of Concern - Workforce (Highlighted in International Work Group)

Risk of operations disruption due to a lack of personnel with in-depth knowledge of complex energy systems and cyber security

Examples:

- *Operators and engineers may not fully understand the cyber security implications of their actions*
- *Personnel may be unable to detect early signs of a cyberattack, hindering rapid response*
- *Skilled personnel are needed to manage legacy industrial control systems effectively*

Consequences:

- *Unintentional system shutdowns or malfunctions due to misconfigurations*
- *Prolonged downtime due to slow resolution of cyber incidents*
- *Increased attack surface for the attackers to exploit*

Capability Focus

- Ongoing activity in region assisting Critical Infrastructure asset owners and operators since 2015
- Hundreds of courses allocated across various gov orgs
- Last 24 months of activity have also focused on regional Workshops

Rapid Response Workshops

15+ Countries
500+ Participants

Joint Team Training Activities

- Ukraine Exercise
- Baltic Region Workshop
- Black Sea Region Workshop
- [Redacted] Workshop
- [Redacted] Workshop
- Belgium Workshop



IT & MGMT

- Forensics
- Threat Hunting
- Offensive Operations
- OSINT



CI/KR & OT

- Critical Infrastructure defense
- State sponsored attacks
- Cyber Sabotage
- Hands on ICS Defense



Thousands of Training Hours

Instructor led training based on in field response experience and hands on labs



Individual Training

Role specific courseware assigned to Ukrainian system defenders

Topic Areas Covered in Workshops

- **Practical Open Source Intelligence Techniques For Defence**
- **Debunking disinformation and finding hate groups with OSINT**

OSINT



- **CTI in times of conflict**

CTI



- **ICS intro, and trends**
- **ICS Defender focused actions**

ICS



- **ICS Security for Leaders and Managers**

MGMT



- **Defending Against State Sponsored Attackers**

SEC



Department of Energy - Rural and Municipal Utility Cybersecurity (RMUC)

Cybersecurity Training for the Utility Workforce

Strengthening the security posture of electric utilities.

- Launched in 2023
- Event held in each of the six NERC regions and beyond
- Three days of training where attendees chose their own adventure
- Joint team training exercise on the final day
- Free for attendees



Roles and Responsibility Training Tracks



I am New to ICS

DAY 1

- ✓ ICS Foundations

DAY 2

- ✓ DOE CyberStrike

DAY 3

- ✓ Team Up & Learn / Share hands-on challenge



I am an ICS practitioner

DAY 1

- ✓ DOE CyberStrike

DAY 2

- ✓ Pick 2 Half-Day Workshops aligned with Job Role

DAY 3

- ✓ Test Your Skills & play as individual against peers



I am a Cybersecurity Professional

DAY 1

- ✓ ICS Foundations

DAY 2

- ✓ Pick 2 Half-day Workshops aligned with Job Role

DAY 3

- ✓ Team Up & Learn / Share hands-on challenge



I am in Leadership

DAY 1

- ✓ DOE CyberStrike

DAY 2

- ✓ OSINT & ICS Leadership Half-day Workshops

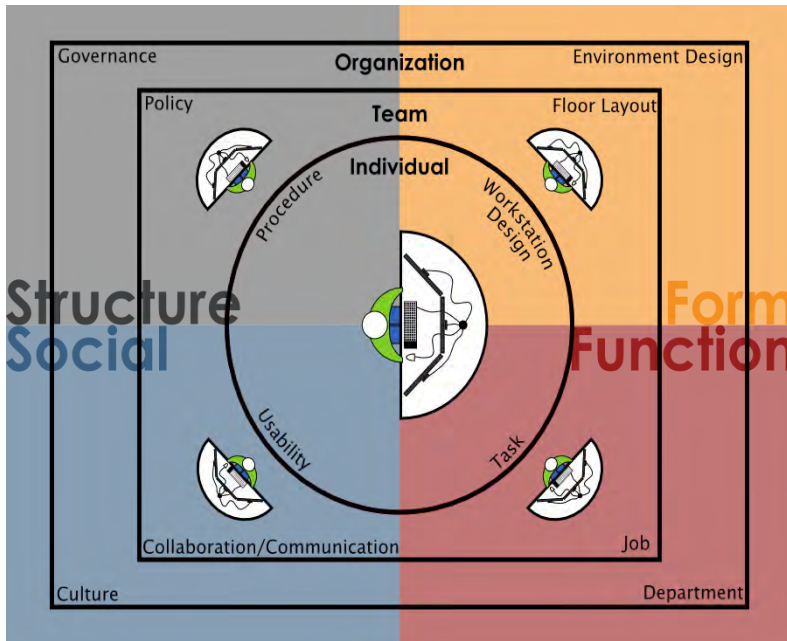
DAY 3

- ✓ Team Up & Learn / Share hands-on challenge

Exercises and Simulation

Practice the way you play

Operations Integrated Cybersecurity Training



- ❑ Complex system under control
- ❑ Multiple operator tools
- ❑ Variety of displays
- ❑ Various alarms and alert screens
- ❑ Distant from the environment under control
- ❑ Rapid decision making required

TTX based training for organization and industry coordinated response

On the Job training & simulation based qualification

Individual knowledge training and certification

Integrated operations, physical, and cyber simulation



Exercise Goals – Learning Opportunities



Standards
Governance
Culture
System Design
System Maintenance
Architectures

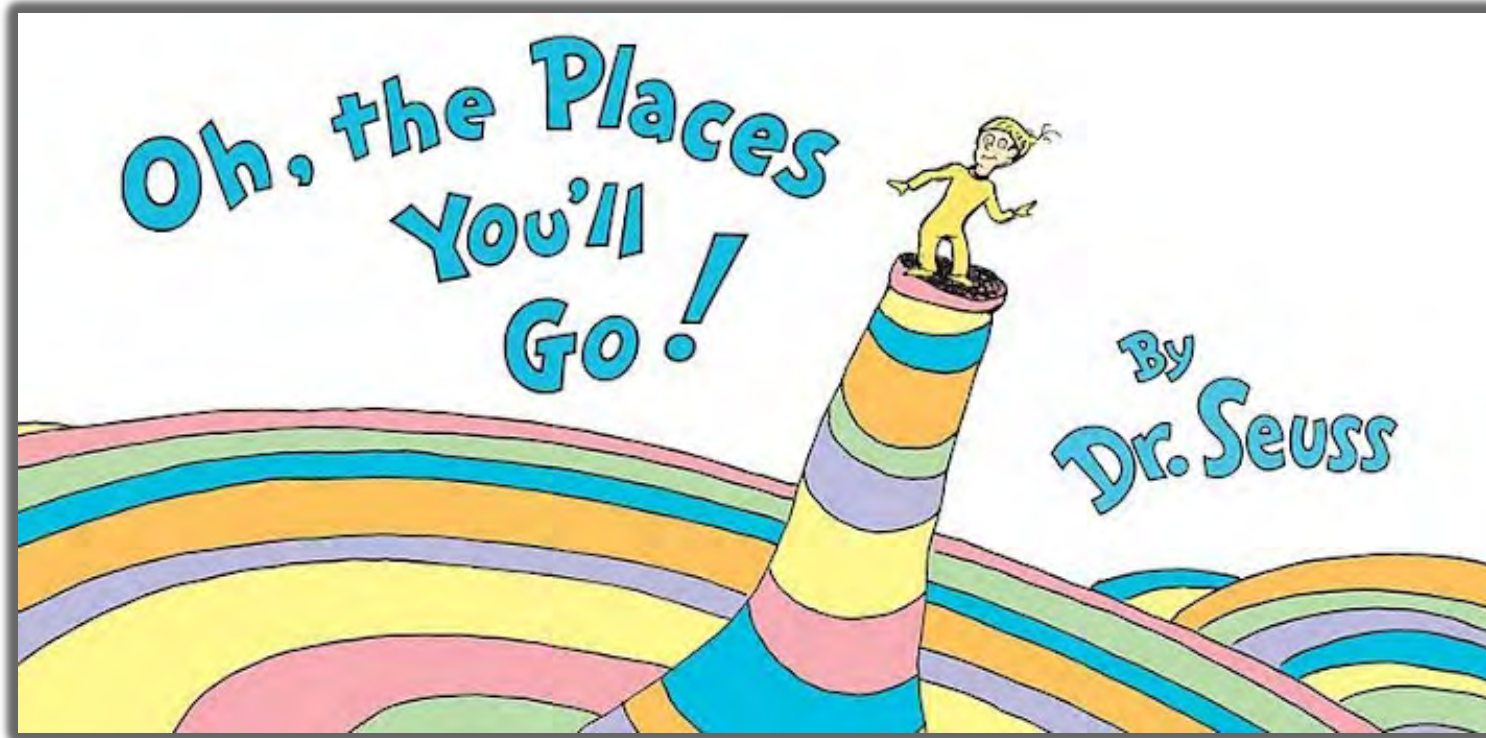


Agility
Defense Capability
Plans
Procedures
Training
Exercises



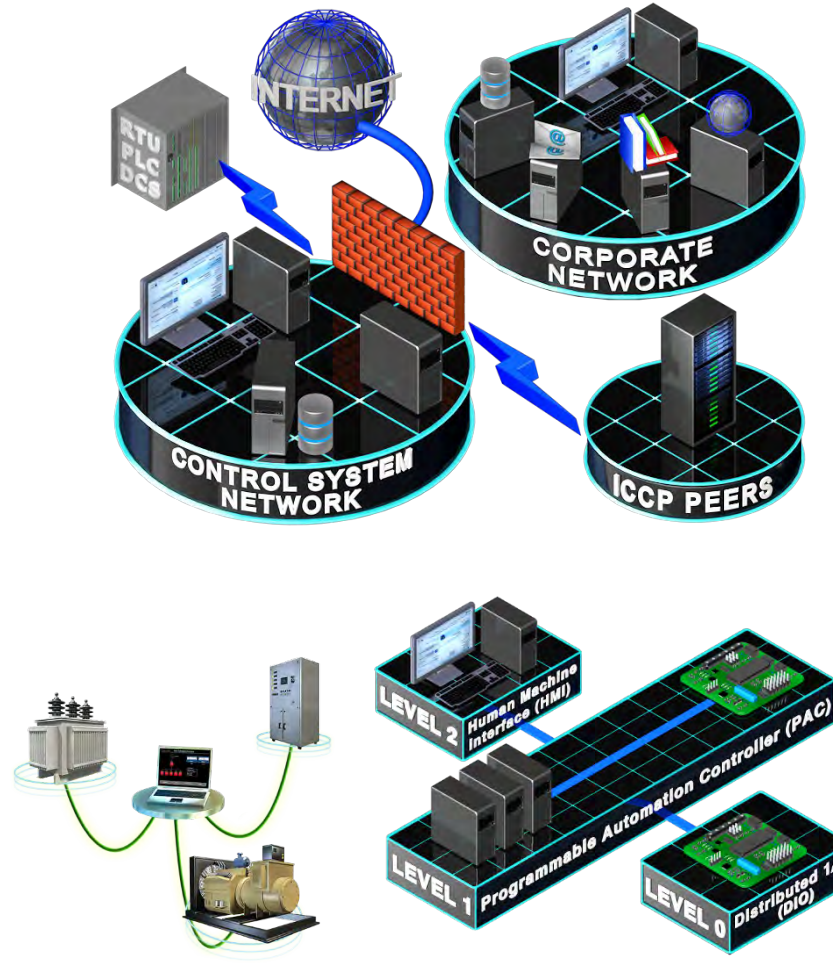
Information Sharing
Law Enforcement
Intelligence
Requests for Assistance
SLA's

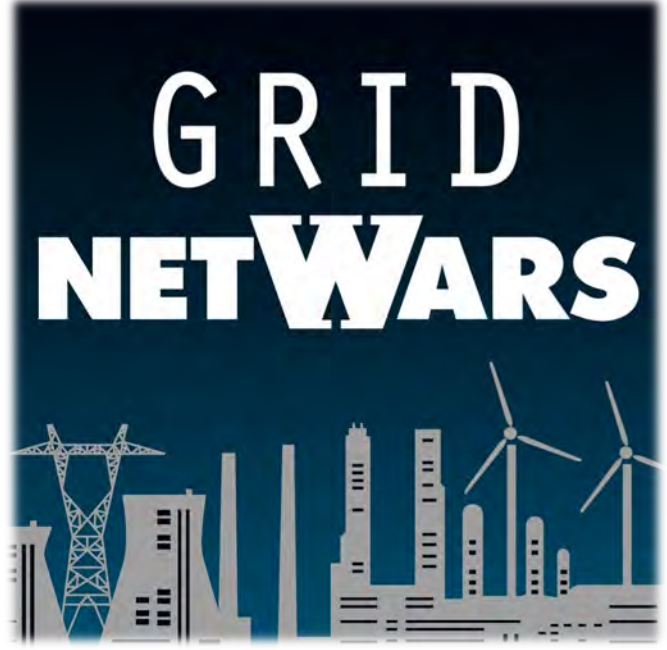
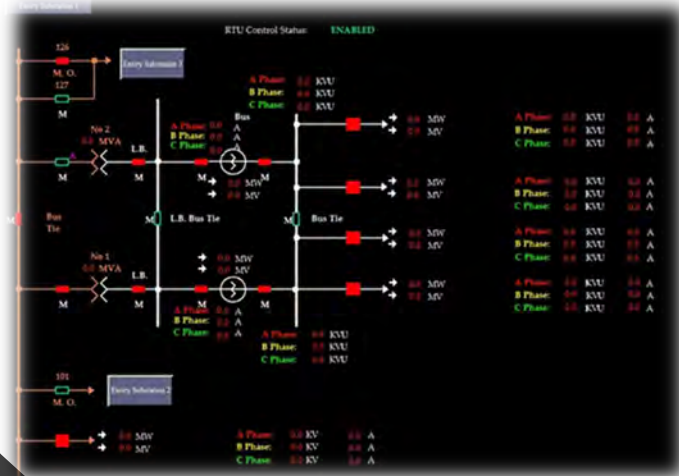
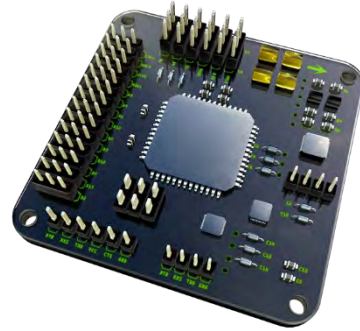
Exercise Goals – Learning Opportunities



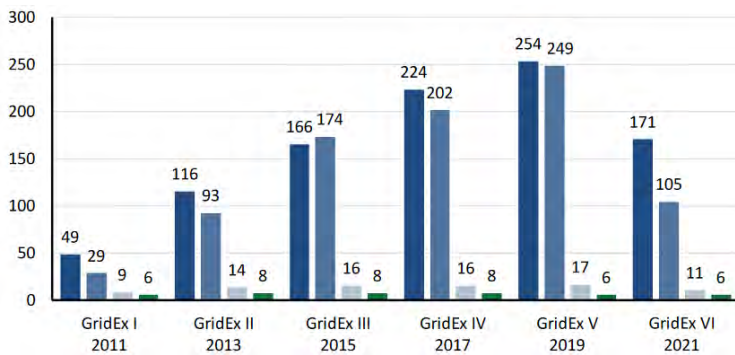
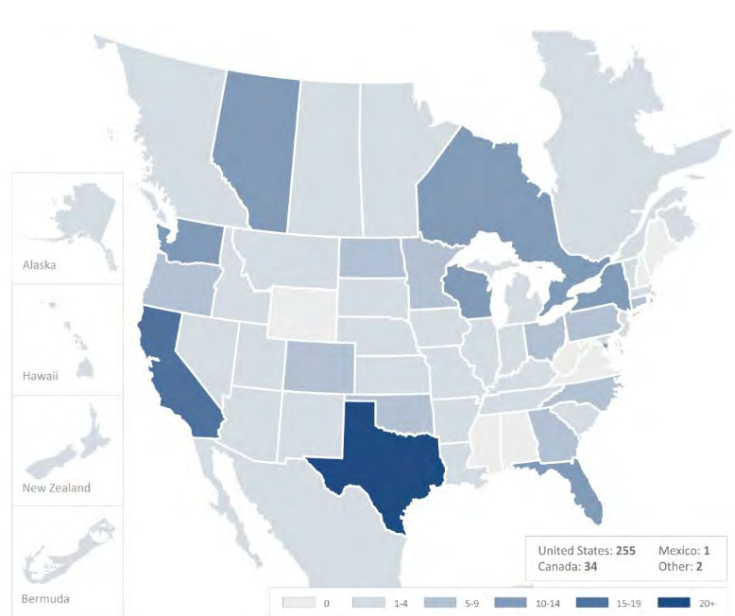
- Interaction and exposure to areas of your organization
- Interaction and exposure to peers
- Education on other sectors
- Learn from others experiences and challenges
- Identify need for response tools and technology

Operational Environment Silos



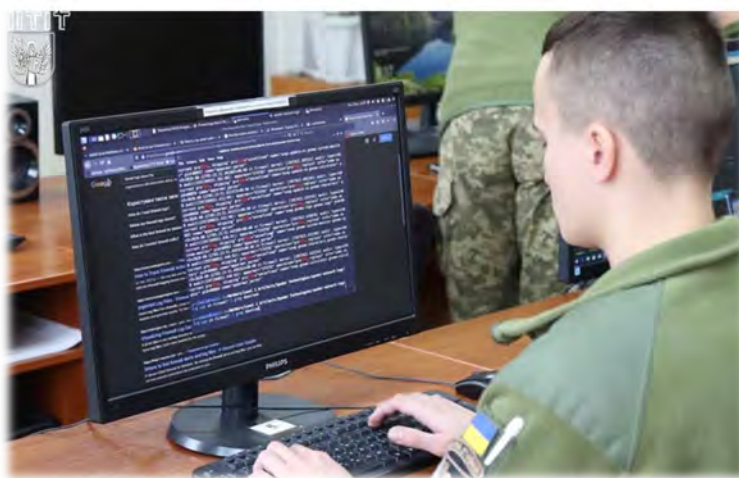
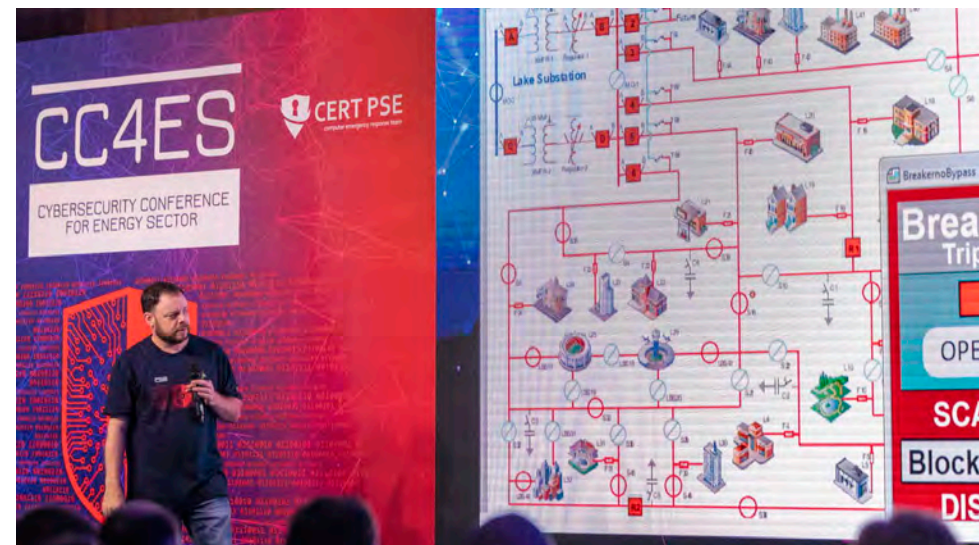


Exercises and Ranges



Команди ВІТІ взяли участь у кібернавчаннях Grid NetWars

Прочитайте за: < 1 жв. 3 Грудня 2021, 16:30



Hands on Elements



POSITION	DISPLAY NAME
1st	2023
2nd	TheOther
3rd	WATER

Muscatatuck Urban Training Center



Parting Thoughts

NERC, DOE, & FERC

Theme 3 - Shortages of Labor and Skillsets



CRITICAL INFRASTRUCTURE PROTECTION

THEMES AND LESSONS LEARNED

MITIGATING RISKS BEHIND THE CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

2024



BY THE NUMBERS

Gap between cyber security workers needed and number available increasing

12.6%

Year over year growth



70%

Of organizations in the energy/power/utilities industry report a shortage of cyber security staff

79%

Of organizations in the energy/power/utilities industry view the current threat landscape as the most challenging it has been in the past five years



Source: ISC2 Cybersecurity Workforce Study (2023)

“The ERO Enterprise often sees noncompliances that result, at least in part, from entities losing skilled labor and failing to successfully transition the underlying job responsibilities to new or existing staff.”

NERC Recommendations

- Utilize existing staff to train and develop others
- Work with HR to reassess competitive salaries to attract and retain
- Ensure adequate resources to execute processes without overly tasking existing staff
- For new technology pursue vendor training prior to implementation
- Implement succession plans for staff who support unique program components
- Identify technology commonalities between departments, BUs, or affiliates
- Leverage ERO provided: training, workshops, webinars, lessons learned resources

C2M2 WORKFORCE Domain – Workforce Management

The Workforce Management (WORKFORCE) domain comprises five objectives:

1. Assign Cybersecurity Responsibilities
2. Develop Cybersecurity Workforce
3. Implement Workforce Controls
4. Increase Cybersecurity Awareness
5. Management Activities

- Cybersecurity responsibilities are assigned to specific people
- **Cybersecurity training is provided as a prerequisite to granting access to assets that support the delivery of the function**
- Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk
- **Adequate resources (people, funding, and tools) are provided to support activities in the WORKFORCE domain**
- The effectiveness of activities in the WORKFORCE domain is evaluated and tracked

FERC Order 893

183 FERC ¶ 61,033
DEPARTMENT OF ENERGY
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 35

[Docket No. RM22-19-000; Order No. 893]

Incentives for Advanced Cybersecurity Investment

(Issued April 21, 2023)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule.

SUMMARY: The Federal Energy Regulatory Commission is revising its regulations to provide incentive-based rate treatment for the transmission of electric energy in interstate commerce and the sale of electric energy at wholesale in interstate commerce by utilities for the purpose of benefitting consumers by encouraging investments by utilities in Advanced Cybersecurity Technology and participation by utilities in cybersecurity threat information sharing programs, as directed by the Infrastructure Investment and Jobs Act of 2021.

Establishing incentive-based rate treatments for utilities' investment in advanced cybersecurity technologies and participation in cybersecurity threat information sharing programs. FERC issued Order No. 893

Training Callouts

c. Commission Determination

134. We decline to adopt an ROE incentive adder, as proposed in the NOPR. We conclude that the Cybersecurity Regulatory Asset Incentive satisfies the statutory obligation to benefit consumers by encouraging investments by utilities in Advanced Cybersecurity Technology and participation by utilities in cybersecurity threat information sharing programs. We believe that expenses, which include cybersecurity assessments, architectural reviews, maturity model evaluations, software subscriptions, monitoring, training, procuring outside services, and cloud computing services, constitute a large portion of overall expenditures for many cybersecurity investments, including cybersecurity threat information sharing programs. We find that the provision of the Cybersecurity Regulatory Asset Incentive alone provides the encouragement that Congress intended without unduly increasing costs on consumers.

Eligible expenses under this incentive include Capital expenses, and operation and maintenance expenses, outside services, implementation costs, network monitoring, training costs, and cloud computing expenses.

Training Callouts (2)

136. The Commission observed that a range of implementation costs associated with cybersecurity investments could be eligible for deferred rate treatment.²⁵⁸ Such costs may include, for example, training to implement new cybersecurity practices and systems. However, the Commission proposed that, to be eligible for the incentive of deferred cost recovery, such training costs must be distinct from costs associated with pre-existing training on cybersecurity practices. The Commission stated that another

capitalized can be considered for deferral as a regulatory asset. Recurring costs may be eligible for deferral as a regulatory asset and may include, for example, subscriptions, service agreements, and post-implementation training costs. Specifically, the

- **Mandatory training is not eligible**
- **Pre-existing training would not be eligible**
- **Training to implement new cybersecurity practices and systems**
- **Recurring costs for post-implementation training**

SANS Free

Learn the Fundamentals of Cyber Security for Free!



Internet Storm Center

Free analysis and warning service to thousands of Internet users and organization



Free SANS Workshops

Hands-on virtual environments that give you the opportunity to dive into



Solutions Forums & Event Tracks

Engage, connect, and learn from invited speakers who



Scholarship

Get training to launch your cyber security career

Over 150 free tools, webinars, summits, CTFs, whitepapers, posters, cheat sheets, training, etc.
<https://www.sans.org/security-resources/>

Free Resources

Learn More



Webcasts



White Papers



Posters and Cheat Sheets



Blogs



Security Policy Templates



Free Tools



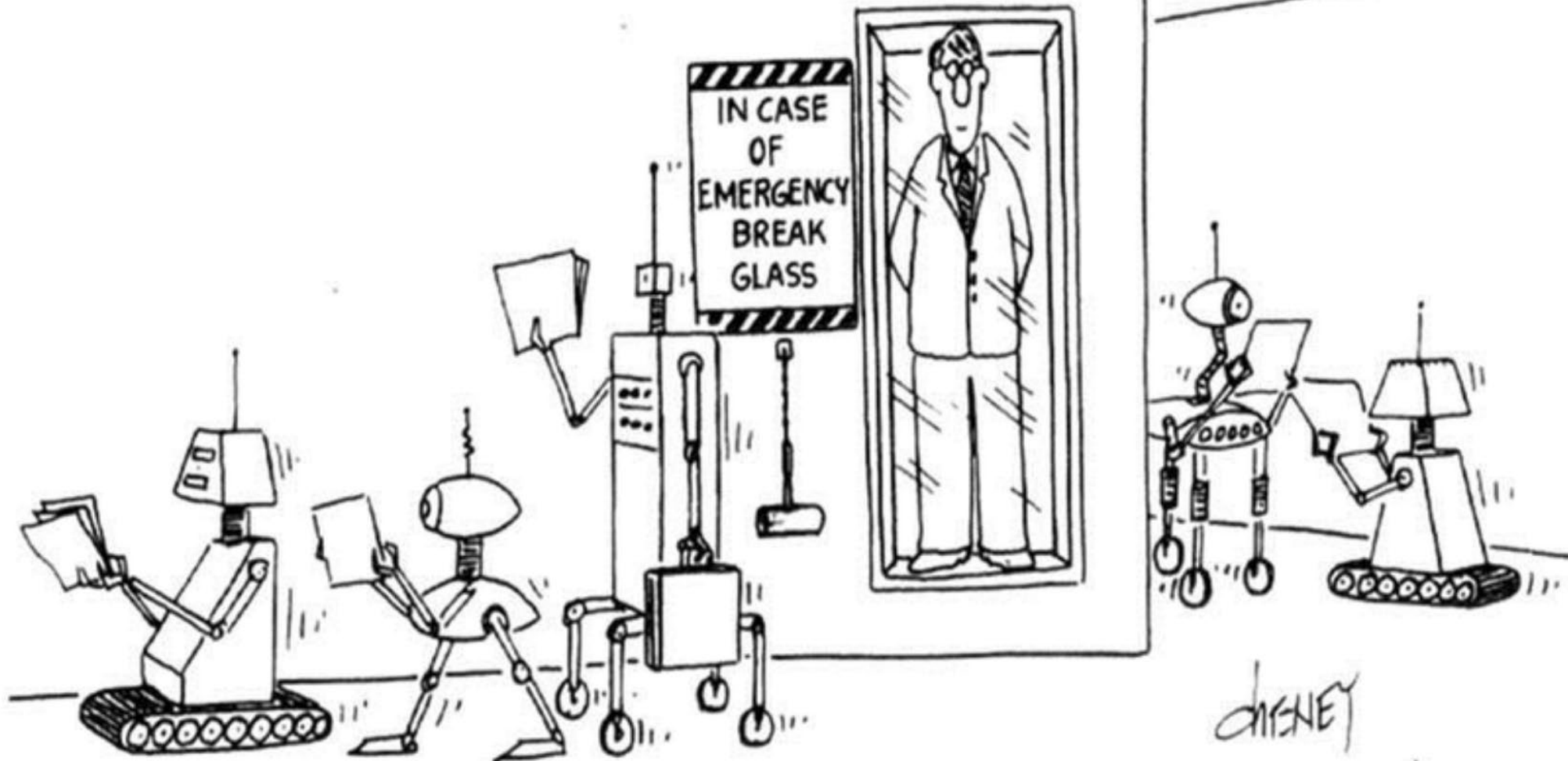
Internet Storm Center



Cyber Security Live Streams

Workforce of the Future – Over Reliance on the Machines

Lew



Q&A



tconway@sans.org

WHAT KEEPS A CSO UP AT NIGHT

FELEK ABBAS

Vice President and Chief Security Officer, SPP





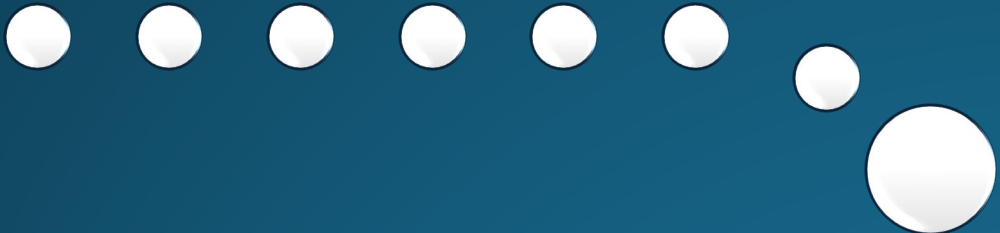
What Keeps a CSO up at Night?

RF FALL RELIABILITY SECURITY SUMMIT

SEPTEMBER 17, 2024

Felek Abbas

Social Engineering



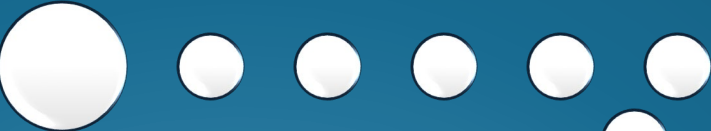
Vulnerabilities



Cloud Computing

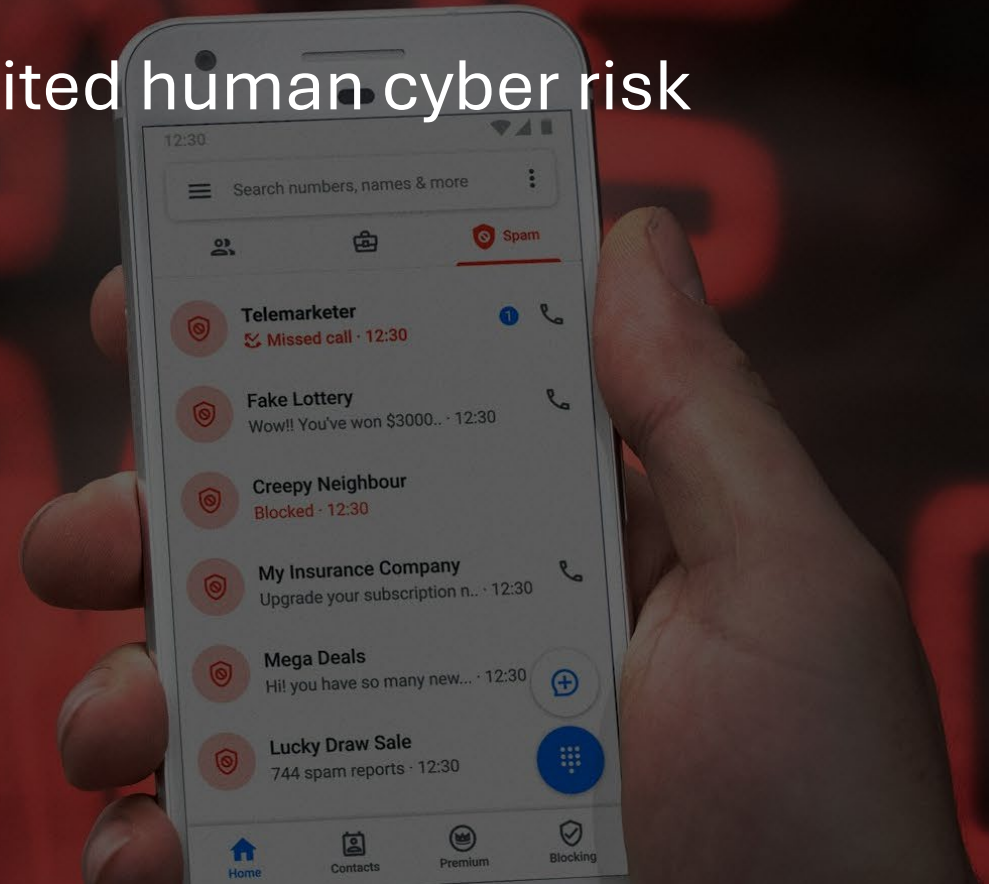


Artificial Intelligence



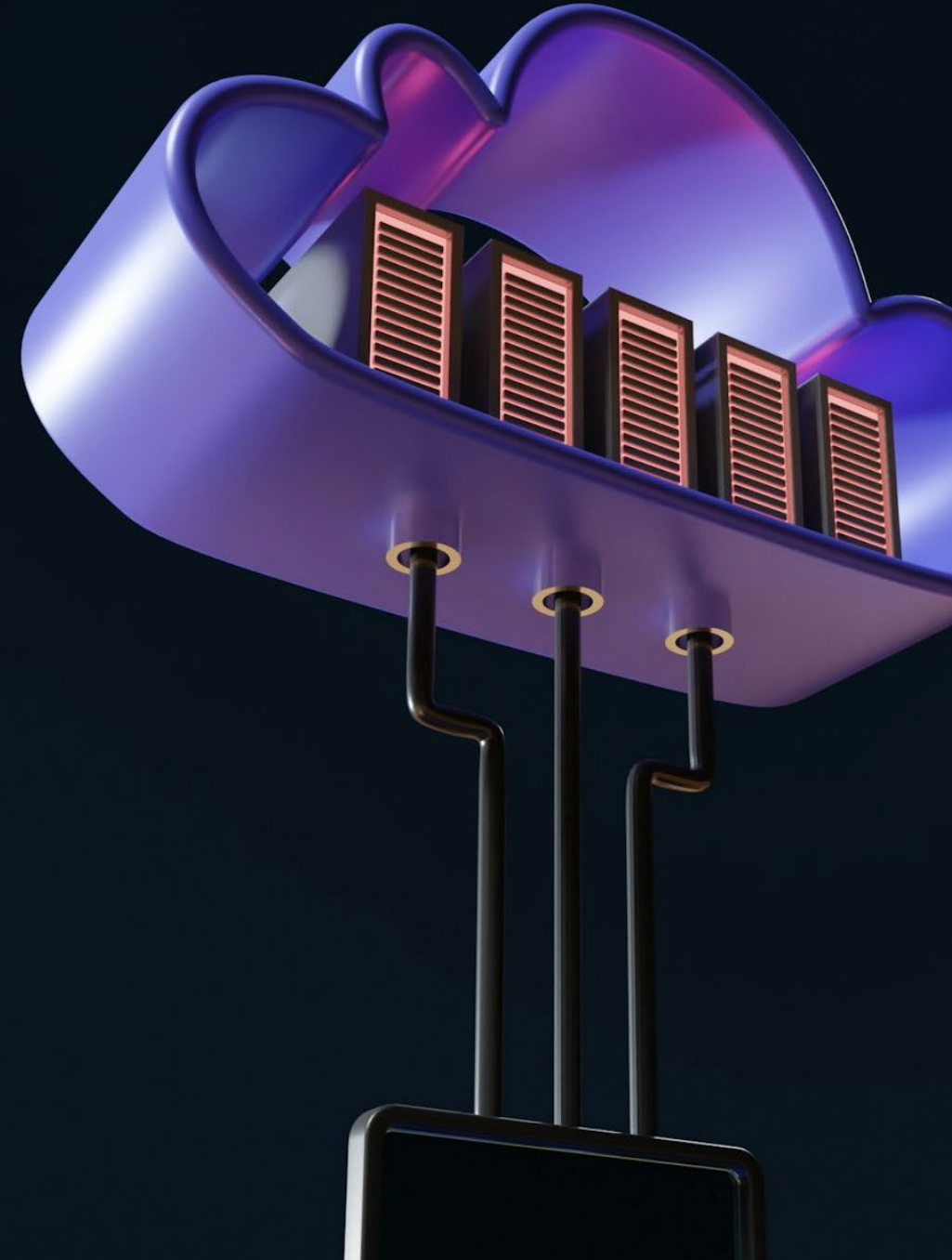
SOCIAL ENGINEERING

- According to SANS survey, this is the top cited human cyber risk
- Preparation
 - Extensive personnel training
 - Rigorous, continual testing
 - Reinforcement
 - Consequences



CLOUD COMPUTING

- Measured approach to cloud
 - What should go in the cloud?
 - Third-party risks
 - Compromises
 - Disruptions
 - Insider threats
 - Ongoing cloud cost (O&M)
 - Cloud exit strategy
 - Cost of repatriating





ARTIFICIAL INTELLIGENCE

- A lot of promise
 - LLMs for complex, dense information processing
 - Simulations and grid planning/management
- Data leakage
- Similar cloud use risks
- Potential for on-prem use

Explosion of Vulnerabilities

- The rate of vulnerability discovery is growing
- The ability of organizations to manage the growth is not scaling
- Looking for more efficiencies to shorten the discovery to mitigation window
 - Automation
 - AI



Please wait while we install a system update

FUNDING

- For utilities, and most organizations, cybersecurity is a necessary cost
- Limited funds are available for most, if not all, organizations tackling threats
- As the critical infrastructure of critical infrastructures, we, as a nation, need to allocate adequate resources to protect the grid
- FERC Order 893
- What about the ISO/RTOs, rural cooperatives, municipalities?
 - We share a joint destiny as interconnected entities on the grid



SOCIOECONOMIC CONSIDERATIONS FOR THE ELECTRIC GRID

JEROME DUMORTIER

Professor and Director of
Research, School of Public and
Environmental Affairs, Indiana
University Indianapolis



INDIANA UNIVERSITY INDIANAPOLIS

[Electricity
Markets,
Land-Use, and
Climate
Change](#)

Dumortier

[Climate
Change](#)

[Past Temperature
Evolution](#)

[Climate Modeling](#)

[Future Climate
Trajectories](#)

[Transport De-
carbonization](#)

[Electric Vehicles
Land-Use Change](#)

[Climate
Change and
Yields](#)

[Research Outlook](#)

[Conclusion](#)

Socioeconomic Considerations for the Electric Grid

Impact of Decarbonization Efforts and Climate Change on Electricity Markets and Agricultural Land-Use

Jerome Dumortier

17 September 2024

ReliabilityFirst (RF) Fall Reliability and Security Summit, Indianapolis, Indiana

Introduction

Short biography

- Ph.D. in Economics from Iowa State University in 2011
- Faculty member at Indiana University Indianapolis since 2011

Research

- Research on agriculture, land-use, and bioenergy since 2009
- Transition of research towards energy more broadly due to interactions between land-use and economy-wide decarbonization efforts
 - ▶ Light-duty vehicle electrification and possibility of bio-based diesel for the freight sector
 - ▶ Sustainable aviation fuels (SAF)
 - ▶ Land requirements for solar and wind farms
- Forward-looking research to inform stakeholders about the impact of future macroeconomic trends, policies, and climate change

Presentation Overview

Past and future evolution of temperature

- Climate modeling and future climate trajectories
- Focus on temperature (as opposed to precipitation) due to its importance for electricity demand

Decarbonization of the transport sector

- Electric vehicles (including Advanced Clean Cars II regulation)
- Sustainable Aviation Fuels (SAF)

Relationship between transport decarbonization and land-use

- Crop yield modeling under climate change
- Land-use effects of climate change and climate change policy
- Impacts on land returns

Short Newspaper Article

“The furnaces of the world are now burning about 2,000,000,000 tons of coal a year. When this is burned, uniting with oxygen, it adds about 7,000,000,000 tons of carbon dioxide to the atmosphere yearly. This tends to make the air a more effective blanket for the earth and to raise its temperature. The effect may be considerable in a few centuries.”

[Rodney and Otamatea Times, Waitemata and Kaipara Gazette, 4 August 1912,
Page 7](#)

Global Surface Air Temperature Anomaly

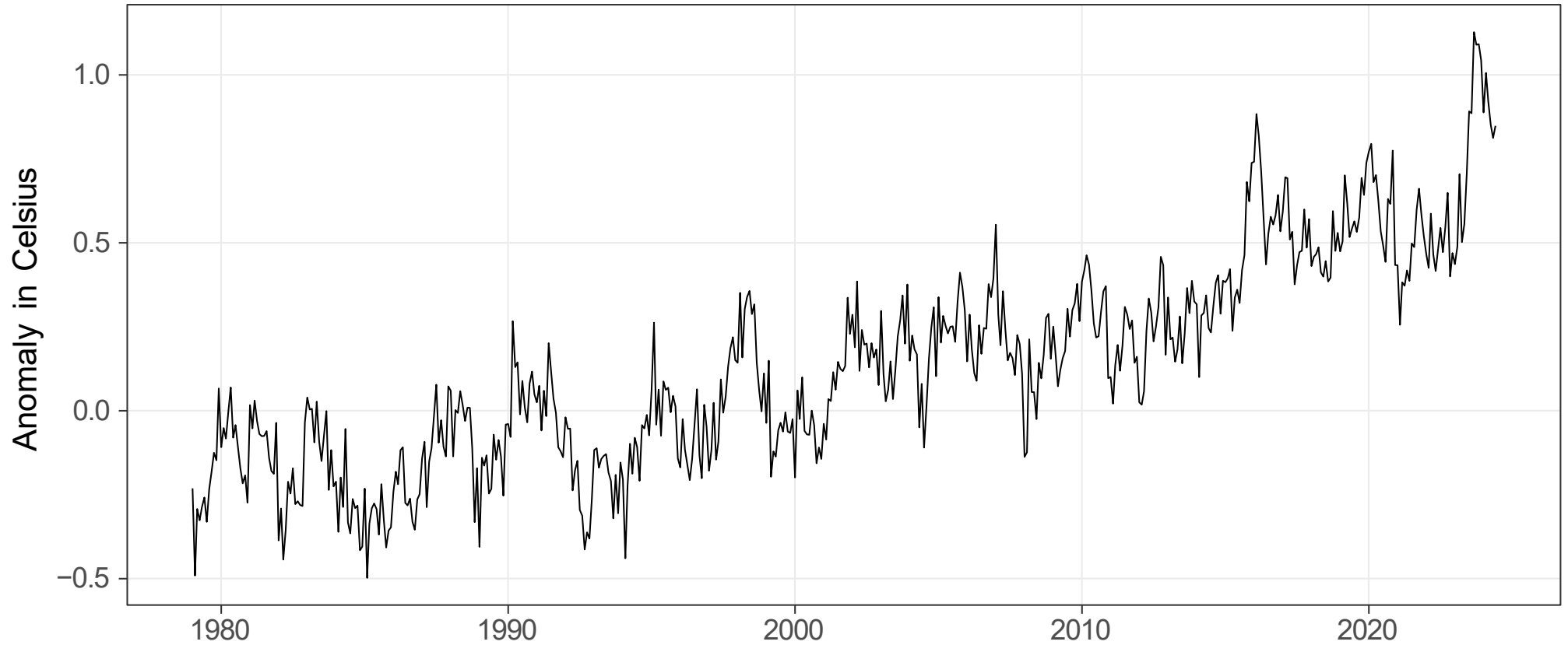
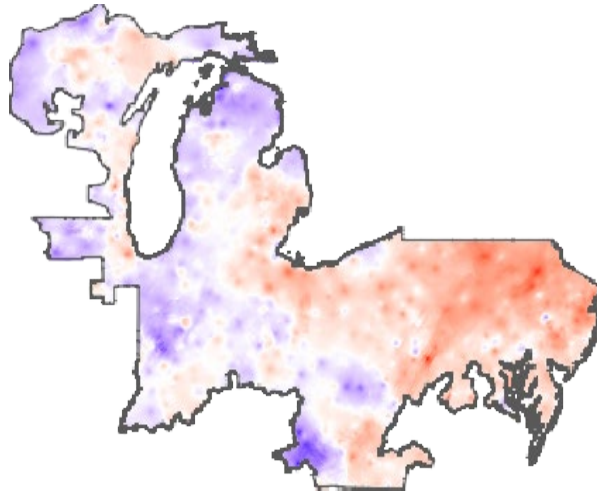


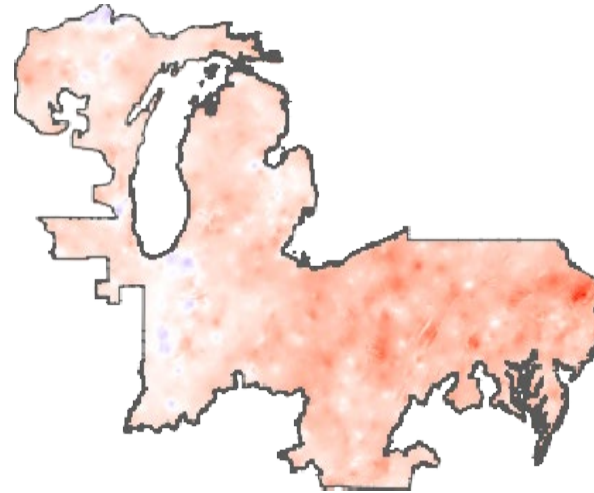
Figure. Global temperature anomaly (January 1979 to June 2024) compared to 1981–2010 mean. Source: [EU Copernicus Programme](#)

Temperature Change for RF Region

(a) Maximum Temperature



(b) Minimum Temperature



(c) Mean Temperature

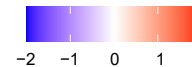
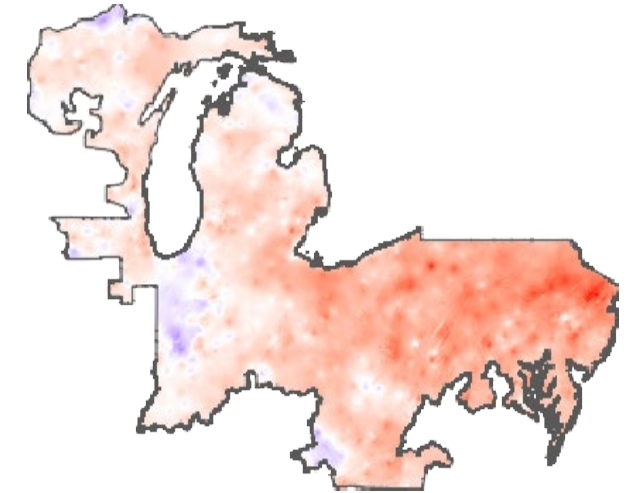


Figure. Change in mean July temperature (in Celsius) between 1981–1990 and 2011–2020. Data Source: [PRISM Climate Group at Oregon State University](#)

Future Climate Modeling

Representative Concentration Pathways (RCP)

- Scenarios representing different greenhouse gas (GHG) concentrations in the atmosphere
- Lower RCP values correspond to lower GHG emissions
- Common RCPs: RCP2.6, RCP4.5, RCP6.0 (current emission trend), and RCP8.5
- Input to climate models

Global Climate Models (GCM)

- Computer models to simulate the behavior of Earth's climate system
- Essential for understanding past climate variability, projecting future climate change, and assessing the impacts of various factors on the climate
- Climate change projections under different GHG emission scenarios

Change in Extreme Temperature Days

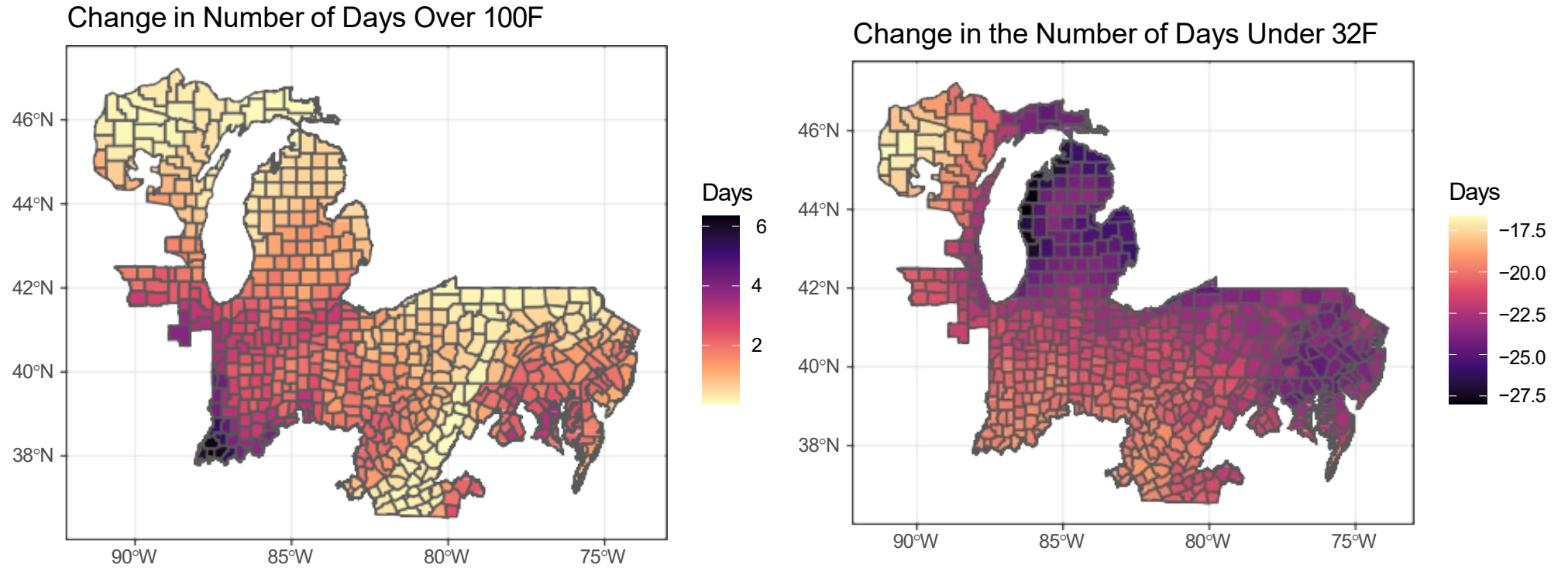


Figure. Change in extreme temperature days under an increase in global temperature by 2 degrees Celsius. Source: [NCA 2023](#)

Changes to Temperature in Marion County

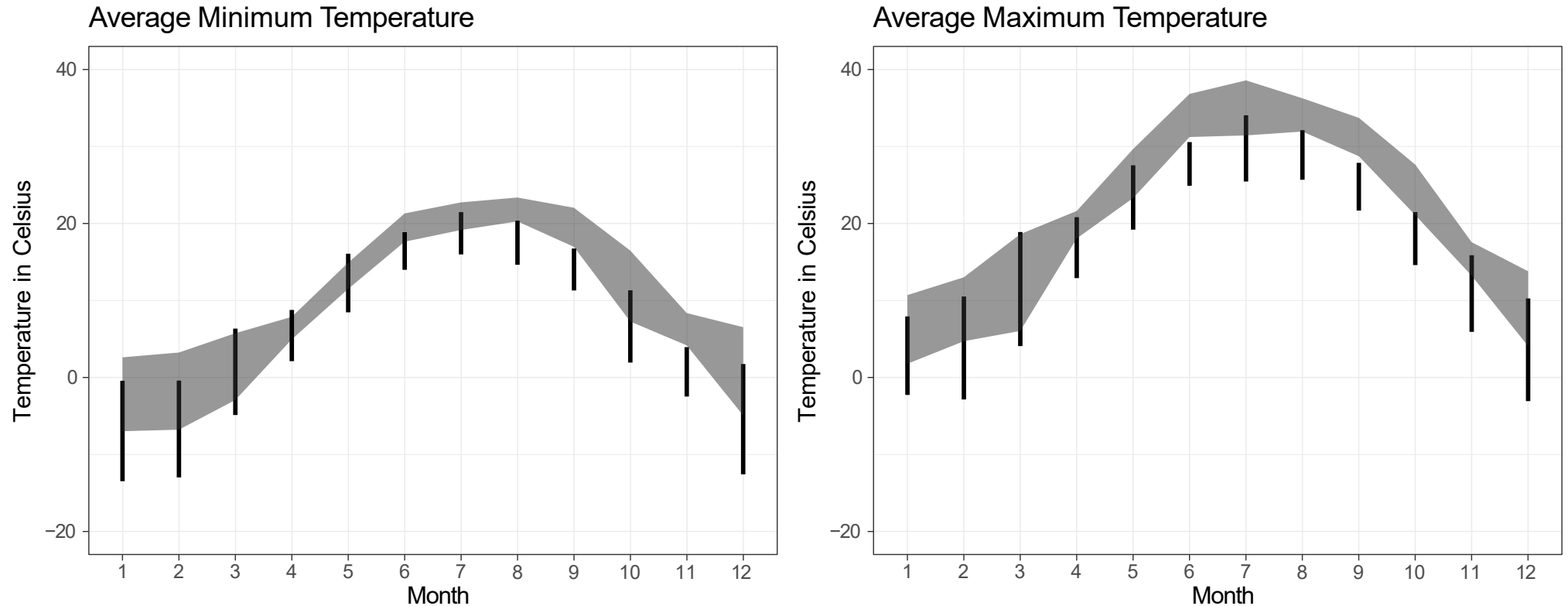


Figure. Solid bars: Average monthly minimum/maximum temperature range 1981–2023. Shaded area: Average monthly minimum/maximum temperature range 2050 under RCP8.5 based on global climate models: GFDL-ESM4, HadGEM3-GC31-LL, HadGEM3-GC31-MM, IPSL-CM6A-LR, MPI-ESM1-2-HR, MRI-ESM2-0, and UKESM1-0-LL.

Increase in ethanol use since mid-2000s

- Corn ethanol as a substitute for MTBE (Methyl-tert-butylether)
- Energy independence and greenhouse gas emissions
- Substitute in the production of gasoline due to high oil prices in 2008
- Consequences: About 1/3 of U.S. corn production for ethanol

Light-duty vehicle electrification

- Long-term decline of ethanol demand due to vehicle electrification
- Implications for farm and consumer welfare as well as land-use and land prices

Sustainable Aviation Fuels

- Multiple feedstocks (besides corn) including soybeans and forest residues

Importance of carbon intensity (CI) scoring for SAFs and (voluntary) carbon markets

Electric Vehicle Market Projections

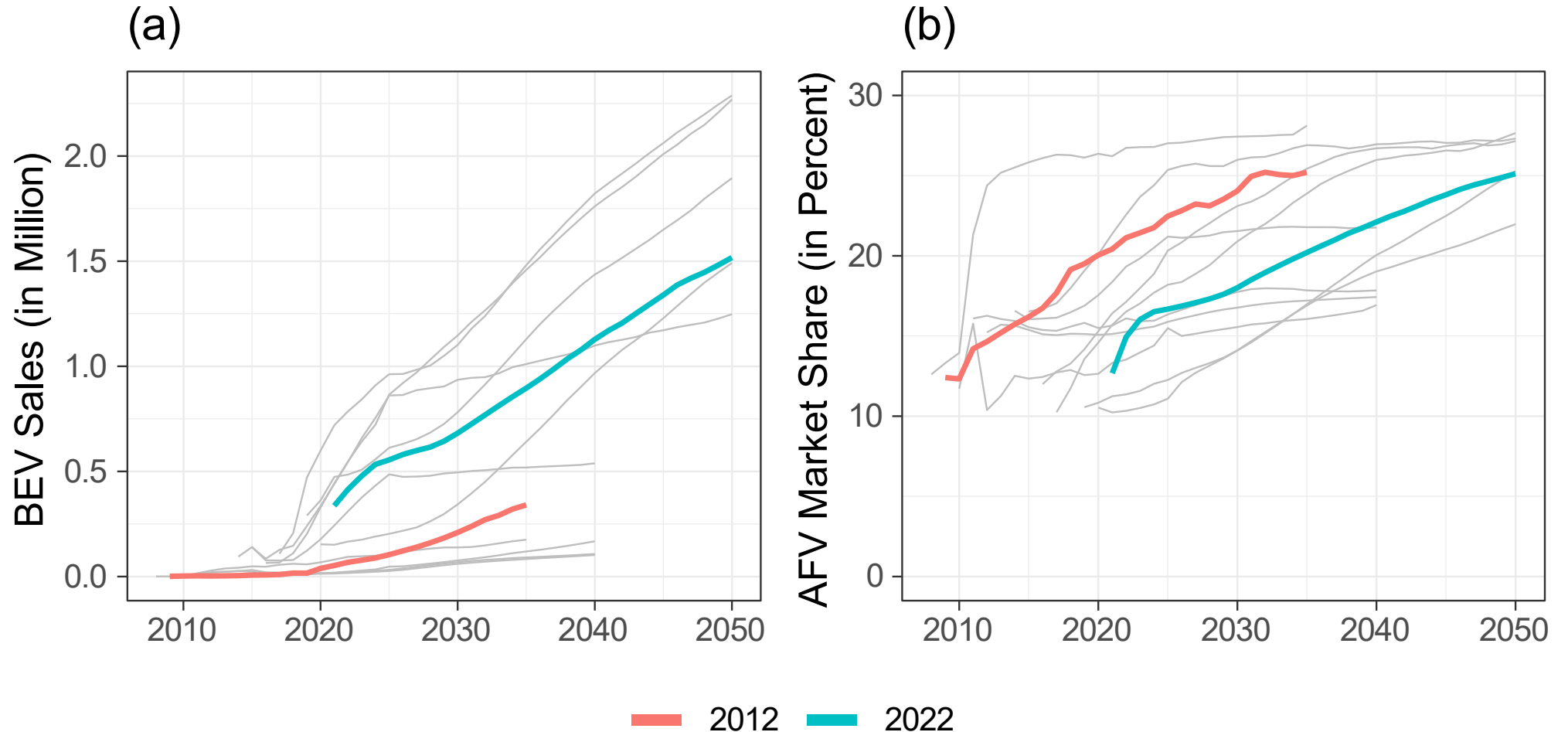


Figure. (a) Battery electric vehicle sales and (b) alternative fuel vehicle market share. Source: 2012–2022 Annual Energy Outlook, U.S. Energy Information Administration

Ethanol Use

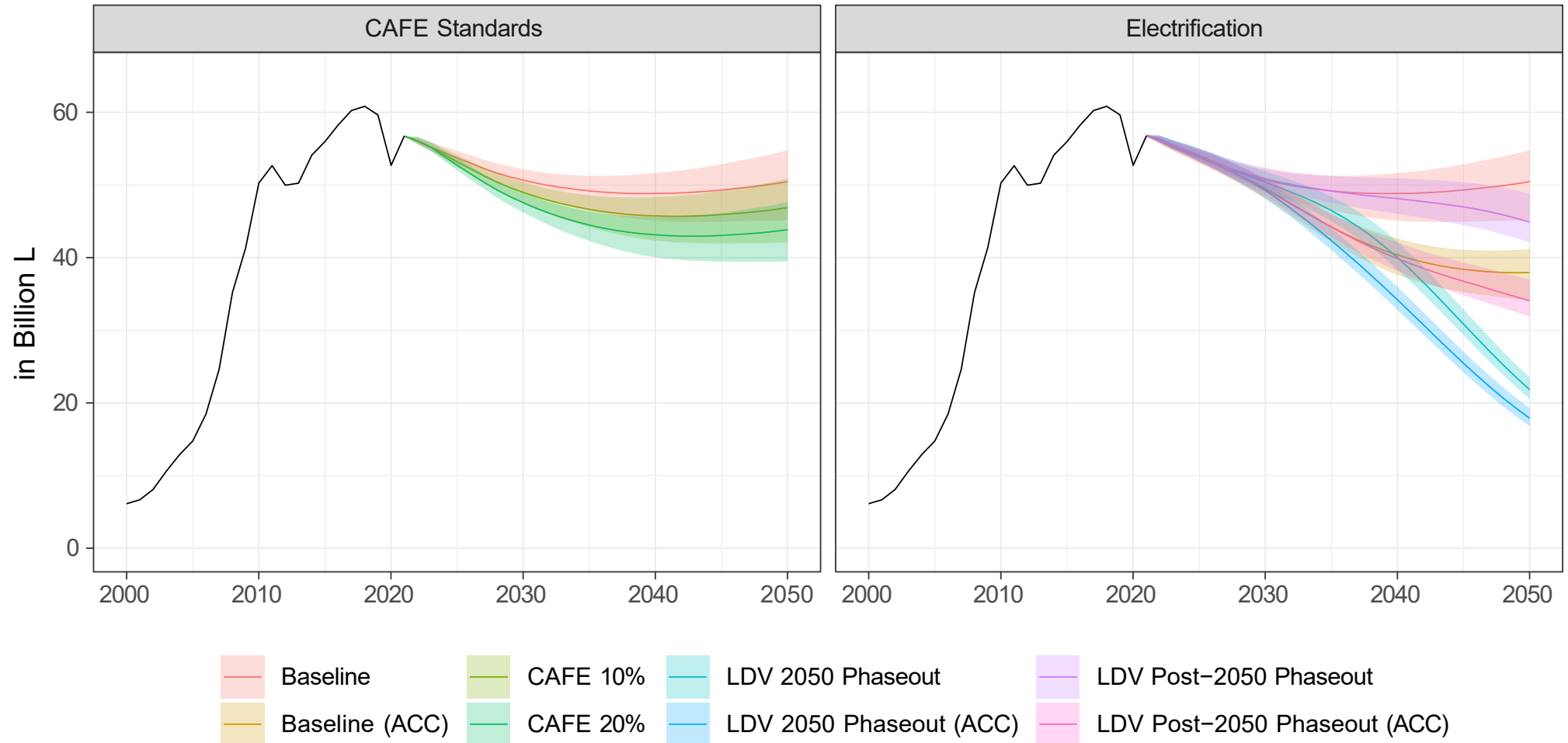


Figure. Historic and projected ethanol use under various Corporate Average Fuel Economy (CAFE) standards and vehicle electrification rates. Source: [Dumortier \(2024\)](#).

Difference in Area

Area Difference: Baseline vs. LDV 2050 Phaseout

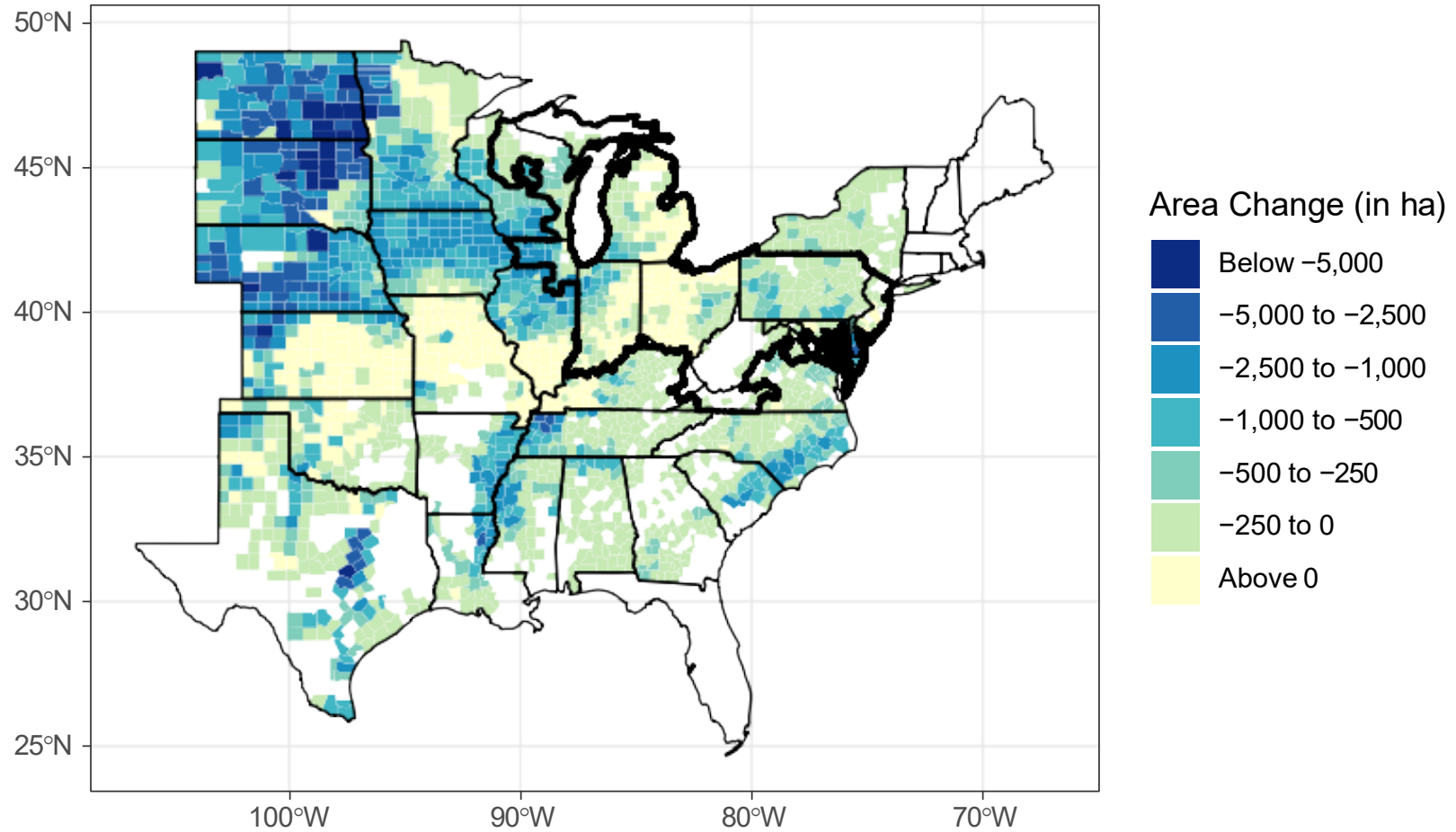


Figure. Difference in area allocation to six crops. Source: [Dumortier \(2024\)](#).

Difference in Profitability

Net Returns Change: Baseline 2050 vs. All 2050 LDV Sales Electric

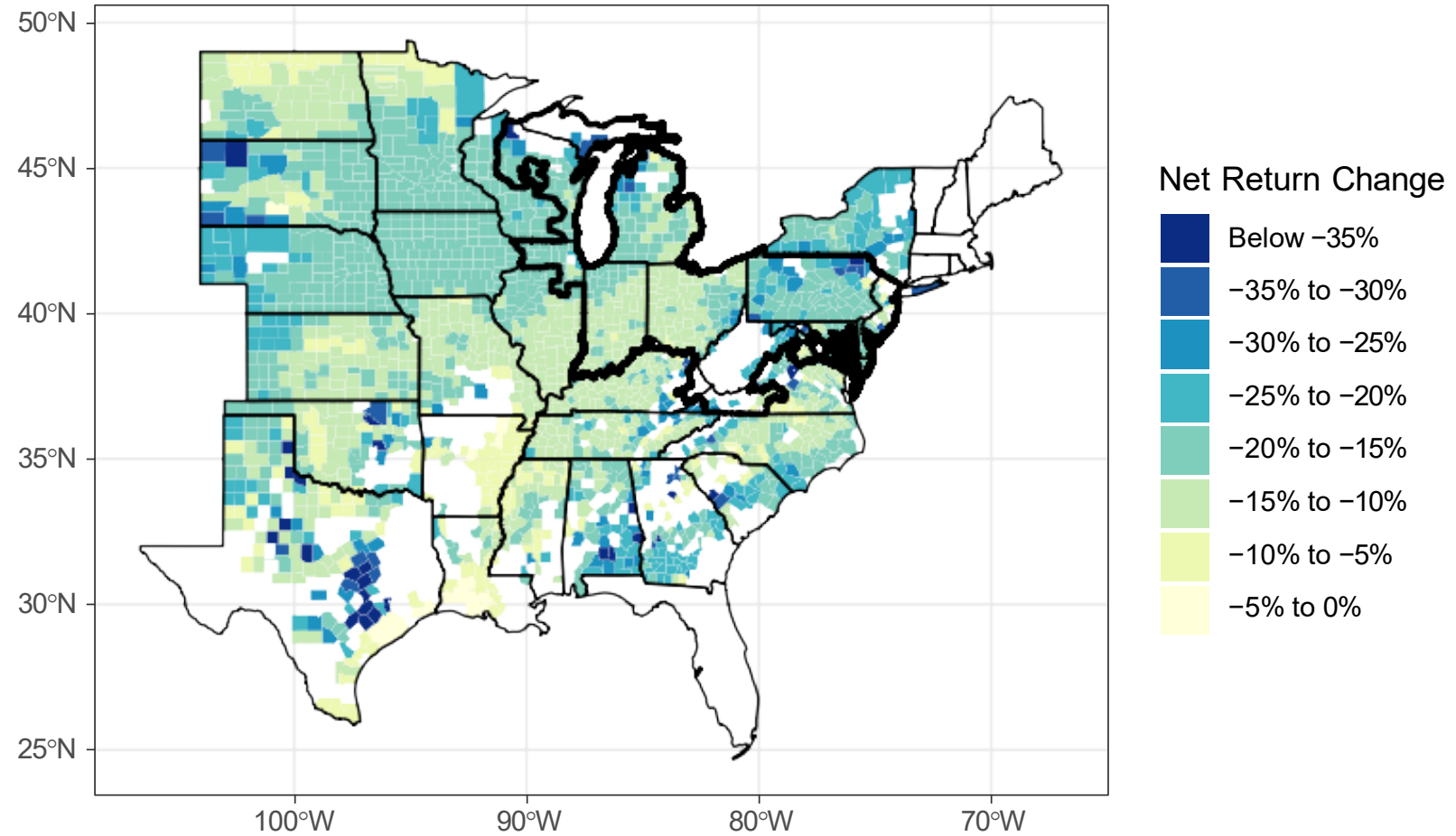


Figure. Difference in net returns from six crops. Source: [Dumortier \(2024\)](#).

Major Unknown Factors

Future rate of electric vehicle adoption

- Expansion of ACC II to potentially other states or drive of electric vehicles by manufacturers

Future of SAFs

- High barriers for corn to qualify for tax credits
- Corn requirements: Adoption of cover crops, no tillage, and enhanced efficiency nitrogen fertilizer
- Tax credits paid to SAF producer but requirements for farmers

Voluntary carbon markets

- Revenue from adoption certain carbon sequestering practices

Positive or negative impact of all unknown factors on land prices

Large-Scale Solar Photovoltaic Installations

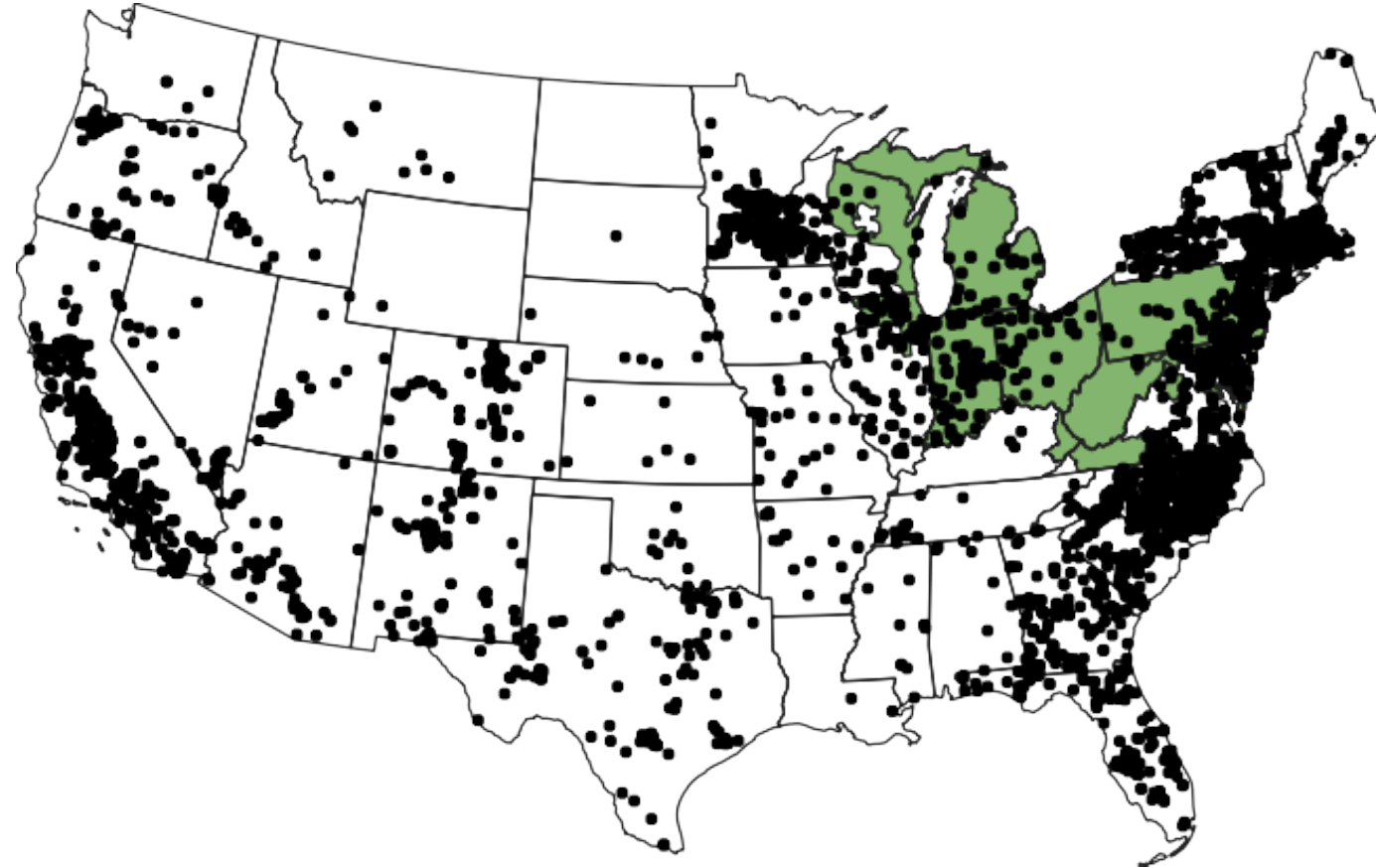


Figure. Current location of large-scale PV installations. Source: [USGS Large-Scale Solar Photovoltaic Database](#).

Yield Changes

Modeling crop yields

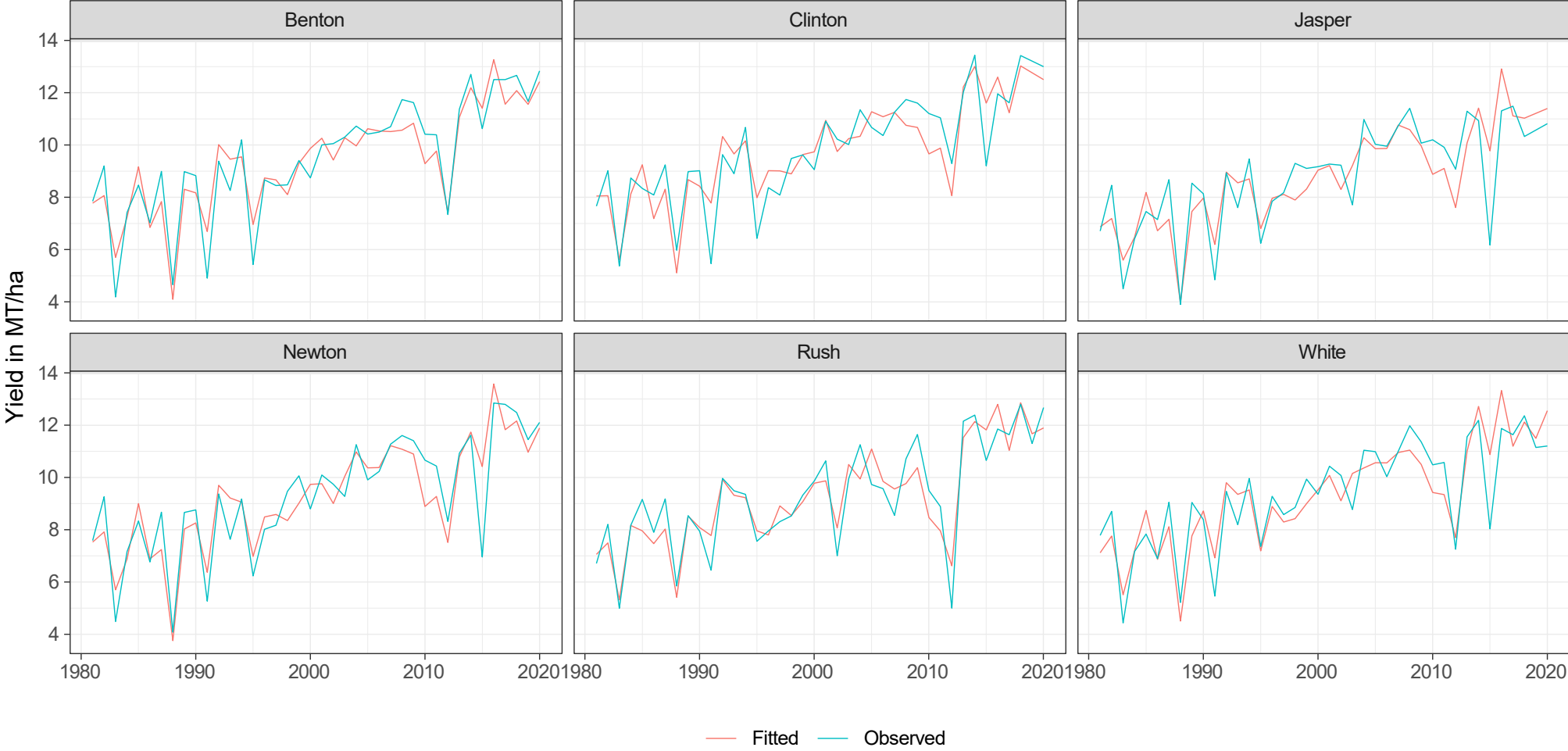
- Statistical models
- Process-based models

Commonly used variables influencing yield

- GDD: Growing degree days as a measure for favorable growing conditions
- HDD: High degree days as a measure for heat stress
- Precipitation as a measure for water availability

Similarity to electricity demand modeling

Corn Yield for Top Producing Counties in Indiana



[Electricity Markets, Land-Use, and Climate Change](#)

Dumortier

[Climate Change](#)

[Past Temperature Evolution](#)

[Climate Modeling](#)

[Future Climate Trajectories](#)

[Transport Decarbonization](#)

[Electric Vehicles](#)

[Land-Use Change](#)

[Climate Change and Yields](#)

[Research Outlook](#)

[Conclusion](#)

Land as an asset playing an important role regarding climate change (policy)

- Revenue from energy production
 - ▶ Currently: Corn ethanol
 - ▶ Future: Potentially corn ethanol but also other feedstock for SAFs
 - ▶ Solar installations
- Revenue from carbon sequestration
 - ▶ Voluntary carbon markets
 - ▶ Feedstock producer for energy sector with carbon intensity scoring requirements

Potentially large impacts of climate change on yields reducing the supply of feedstock

MISO RELIABILITY IMPERATIVE

TODD HILLMAN

Senior Vice President and Chief
Customer Officer, MISO





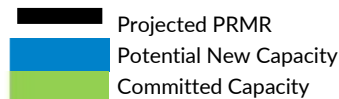
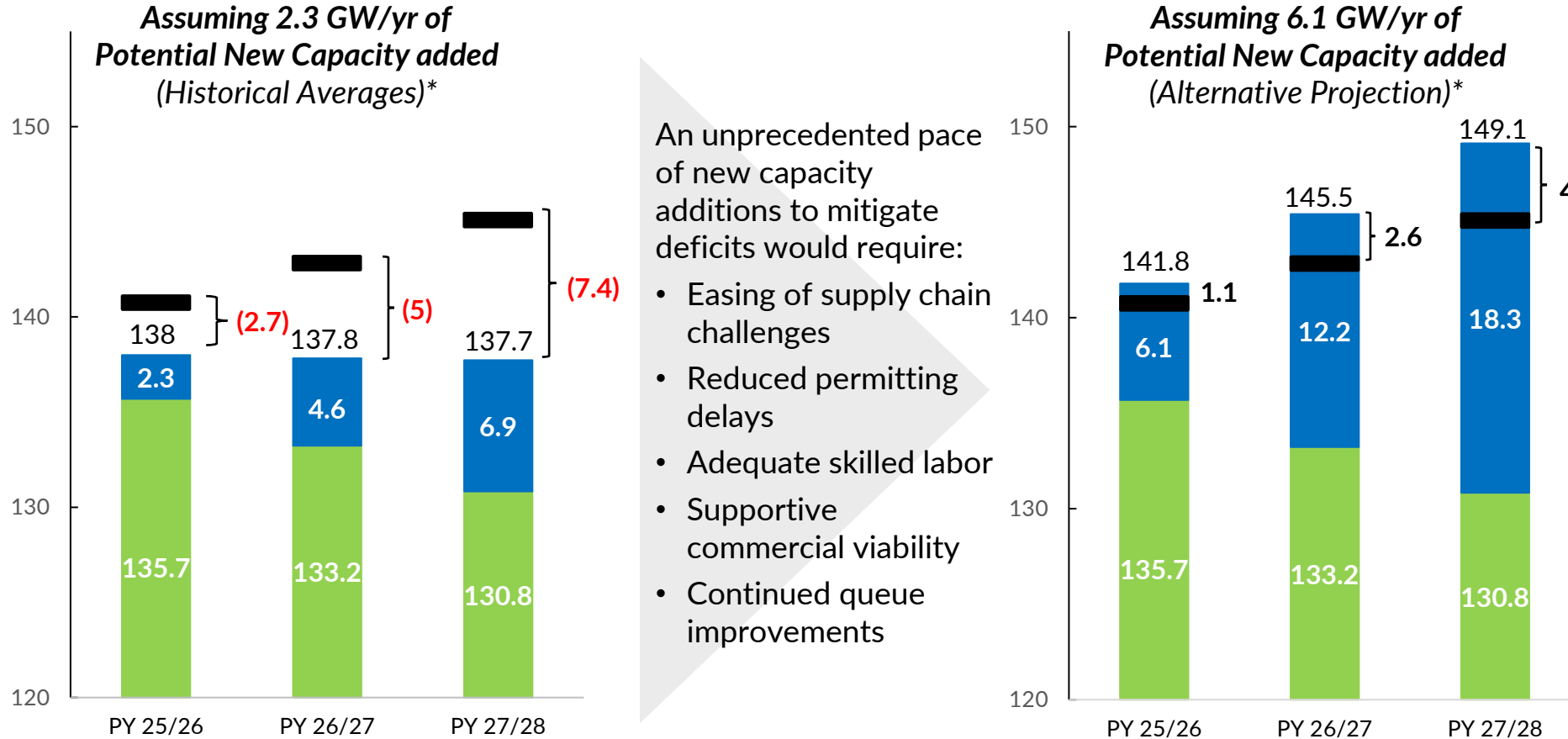
ReliabilityFirst Fall Reliability & Security Summit

MISO Reliability Imperative

September 17, 2024

2024 OMS-MISO Survey indicates increasing capacity deficits requiring a dramatically accelerated pace of new build to mitigate

OMS - MISO Survey Resource Adequacy Projections – Summer (Accredited GW)



- Bracketed values indicate difference between Committed+ Projected New Capacity and projected LSE PRMR
- Capacity accreditation values and PRM projections based on current practices
- Regional Directional Transfer (RDT) limit of 1,900 MW is reflected in this chart

PRMR: Planning Reserve Margin Requirement All references to capacity indicate Seasonal Accredited Capacity (SAC)

* Using methods for Potential New Capacity described in 2024 OMS-MISO Survey presentation

Capacity trends of our RTO neighbors point to declining availability of supportive transfers

PJM

Significant year-over-year supply/demand changes resulted in record prices in capacity auction for 2025/26 delivery year

Offered Supply: - 13.3 GW (down 8.8% vs. prior year)

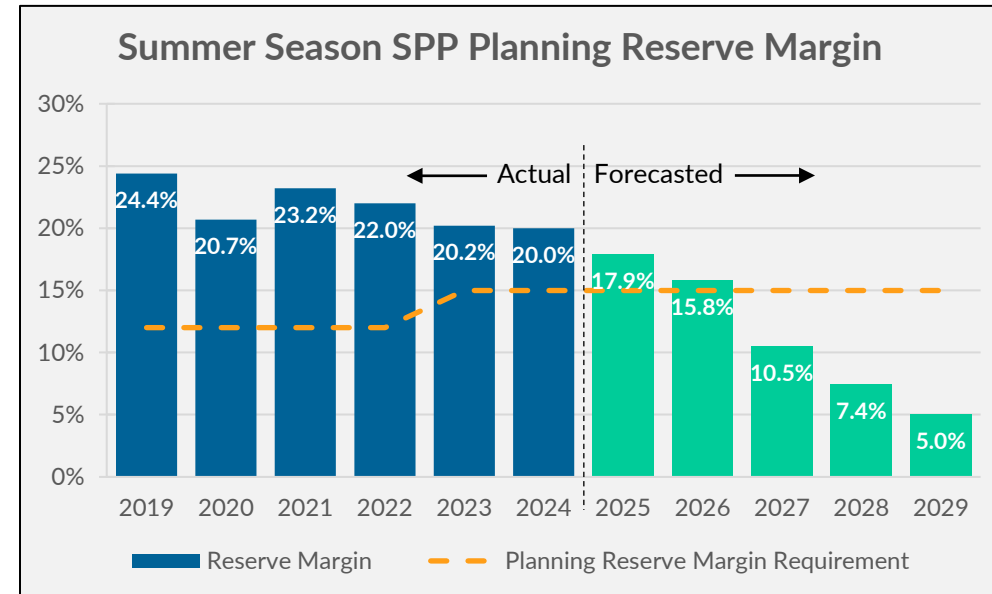
Load: + 3.2 GW (up 2% vs. prior year)

Reserve Margin: 0.7% (vs. 5.4% in prior year)

Clearing Price: ~ \$270 / MW-day (vs. ~\$29 in prior year)

SPP

No capacity auction but reserve margin projected to fall to requirement in 2026 and decline further



Excess capacity of 2,750 MW in 2024 becomes a deficit of 5,950 MW in 2029 due to:

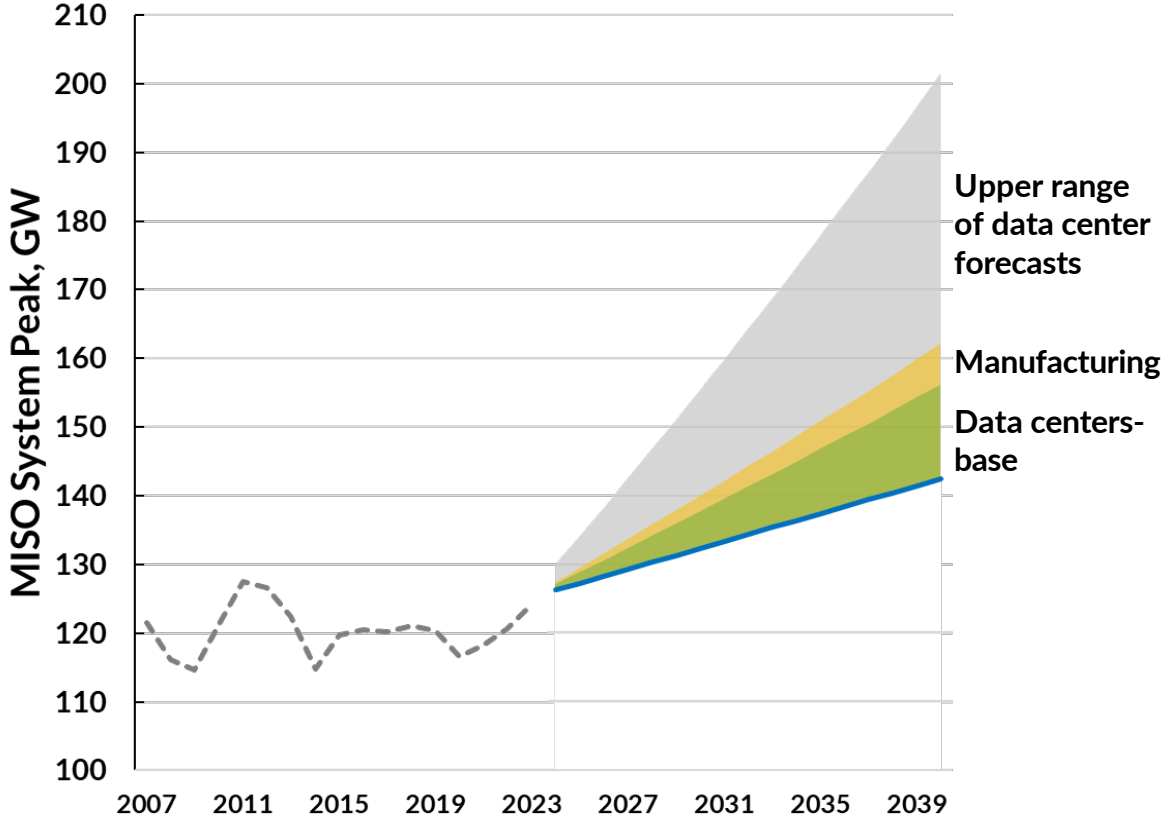
- 10% increase in forecasted demand
- 3% reduction in capacity

Source: PJM 2025/2026 Base Residual Auction Report

Source: 2024 SPP Resource Adequacy Report

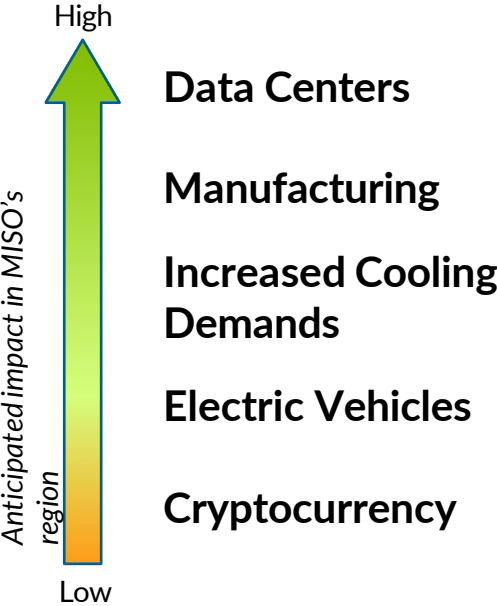
Poor visibility into the magnitude/timing of large load additions is putting at risk our ability to reliably accommodate them

EPRI and Grid Strategies¹ anticipate manufacturing growth to favor MISO's service area



Notes: All figures shown are PRELIMINARY

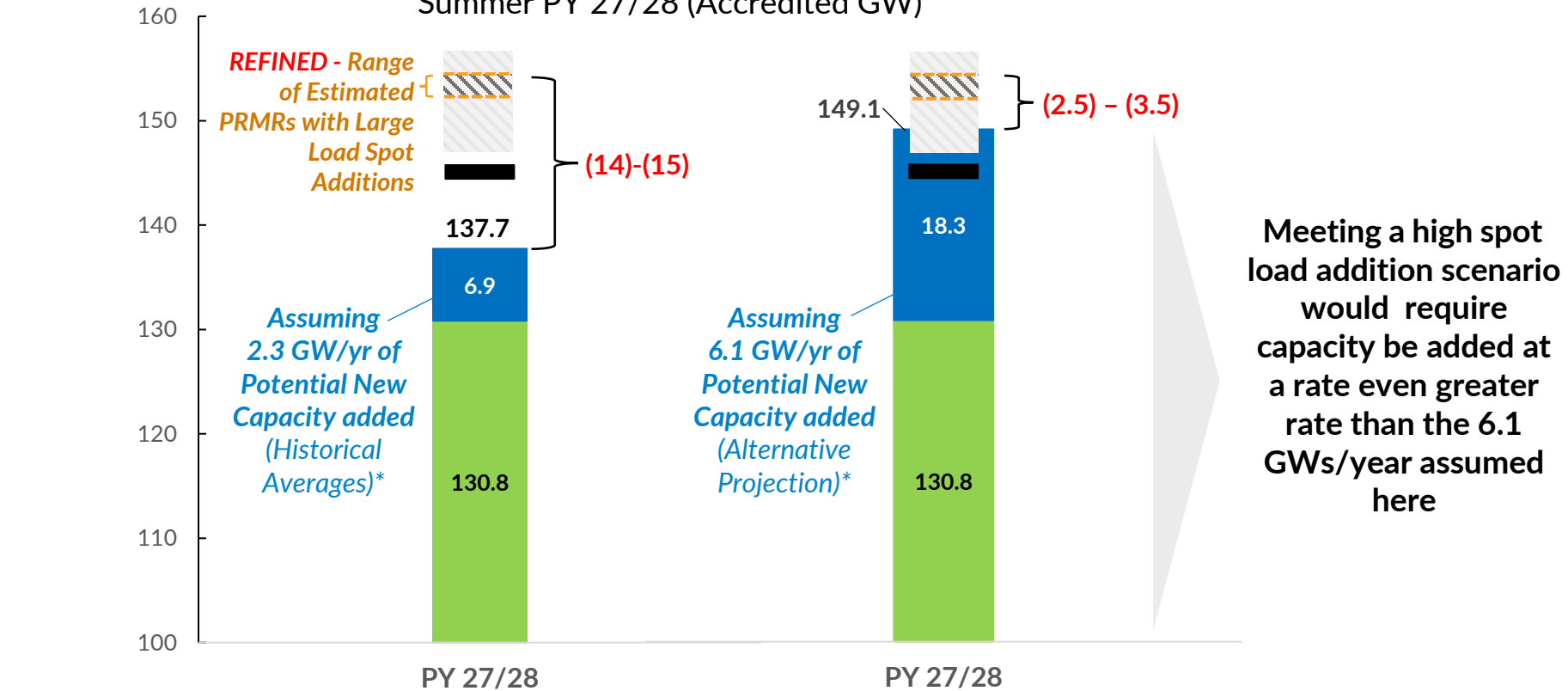
- Grid planners nearly *doubled* their 5-year peak load growth forecasts since last year
- MISO anticipates strong *long-term* load growth driven primarily by:



<https://www.epri.com/research/products/000000003002027930> <https://gridstrategiesllc.com/wp-content/uploads/2023/12/National-Load-Growth-Report-2023.pdf>

The trend of announced large load additions will exacerbate the urgency for new generation, including dispatchable, long-duration resources

MISO Resource Adequacy Projection vs.
 an Expanded Range of Future Large Load Spot Additions*
 Summer PY 27/28 (Accredited GW)



- REFINED** Range of Estimated PRMRs with Large Load Spot Additions
- ORIGINAL Range of Estimated PRMRs with Large Load Spot Additions
- Projected PRMR with LSE load forecast
- Potential New Capacity
- Committed Capacity

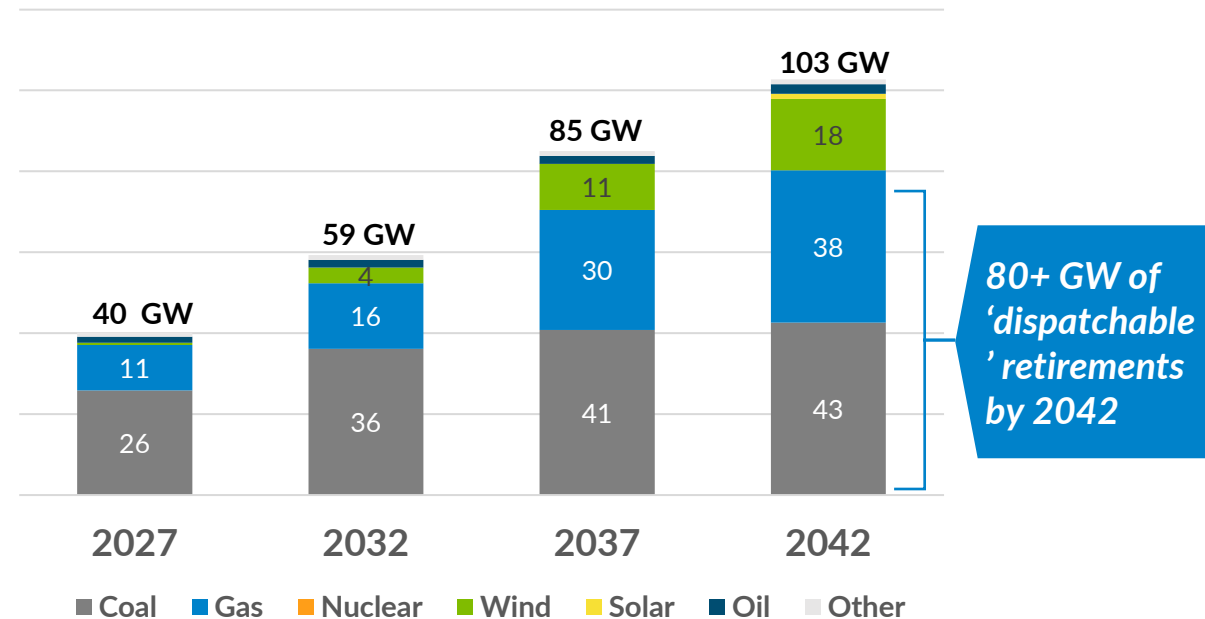
- Bracketed values indicate difference between Committed + Projected New Capacity vs. Projected PRMR with large spot-load additions
- Capacity accreditation values and PRM projections based on current practices
- Regional Directional Transfer (RDT) limit of 1900 MW is reflected in this chart

* Using methods for Potential New Capacity and Large Load Spot Additions described in 2024 OMS-MISO Survey presentation
 PRMR: Planning Reserve Margin Requirement

Policy direction is accelerating thermal unit retirements and increasing the headwinds to new thermal unit development

- Member/state clean energy and decarbonization goals
- U.S. Environmental Protection Agency (EPA) regulations:
 - Carbon Rule
 - Good Neighbor Rule
- Inflation Reduction Act and Infrastructure Bill

Future 2A Total Retirements
(Cumulative GW)



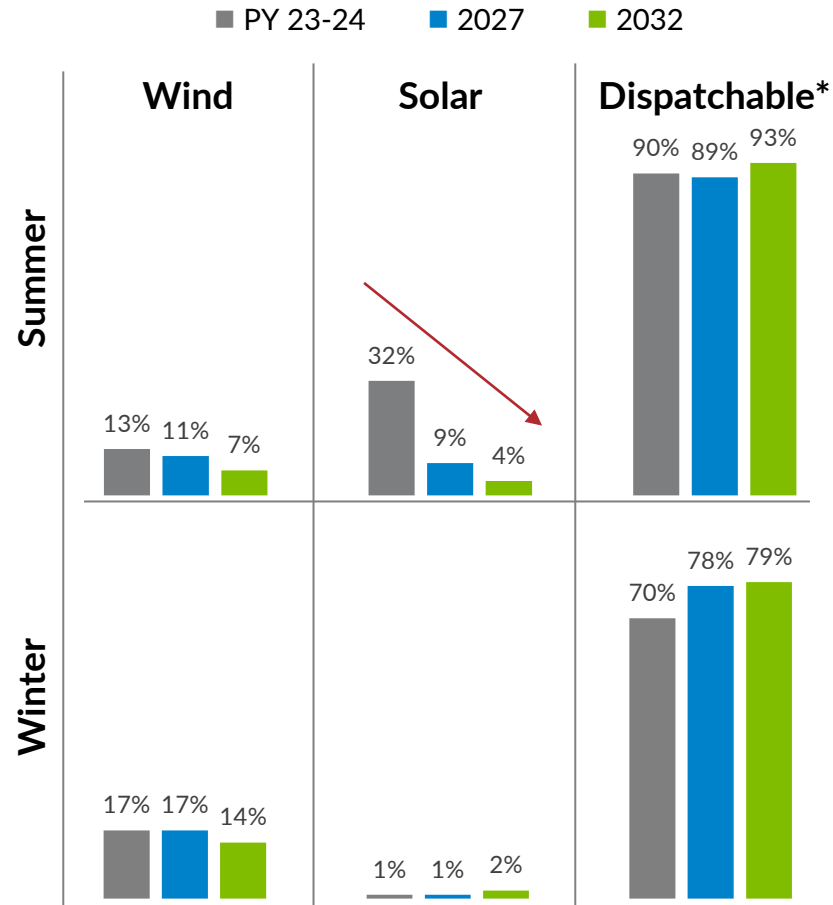
MISO will need to assess Futures to determine if recent developments, especially related to the Carbon Rule, will limit existing resources and may cause additional retirements beyond those assumed here

Filed accreditation changes designed to improve alignment with the reliability value of resources

Approach

- Risk hours expanding from summer peak to also include winter
- Seasonal marginal value based on 'Direct Loss of Load' (DLOL) approach matches accreditation with risk hours based on class and individual asset performance
- Solar accreditation falls off with higher levels of penetration because risk hours are shifted to early evening

Indicative Accreditation Trends (% of installed capacity)



Expected Outcomes

Accreditation based on reliability contribution is the right direction, but it comes with additional coordination challenges as MISO Members evolve their fleets

* Includes coal, gas, nuclear, hydro, pumped storage, etc.

MISO has made considerable progress on evolving our processes and tools to support resource adequacy, but additional coordination can drive more efficient and effective resource planning

Recently Completed / In-Process

Initiative	Objective
Seasonal Requirements in Planning Resource Auction	More accurately reflect variations in resource capabilities and availability
Accreditation Enhancements	Improve alignment of capacity “value” with reliability contribution
Reliability-Based Demand Curve	Improve price signals for capacity and inform investment decisions
Shortage Pricing	Incentivize market participant real-time behavior and actions to avoid potential shortage situations

Next Opportunity

- As the fleet continues to evolve, visibility and clarity will be critical to support timely and prudent action.
- MISO processes and assessments provide insights into the region’s short- and long-term supply and demand picture:

Planning Resource Auction	1 Year
OMS-MISO Survey	5 Years
Regional Resource Assessment	20 Years
MISO Futures	20 Years

- A recent stakeholder survey uncovered a desire to evaluate streamlining MISO’s assessments, which may improve participation.

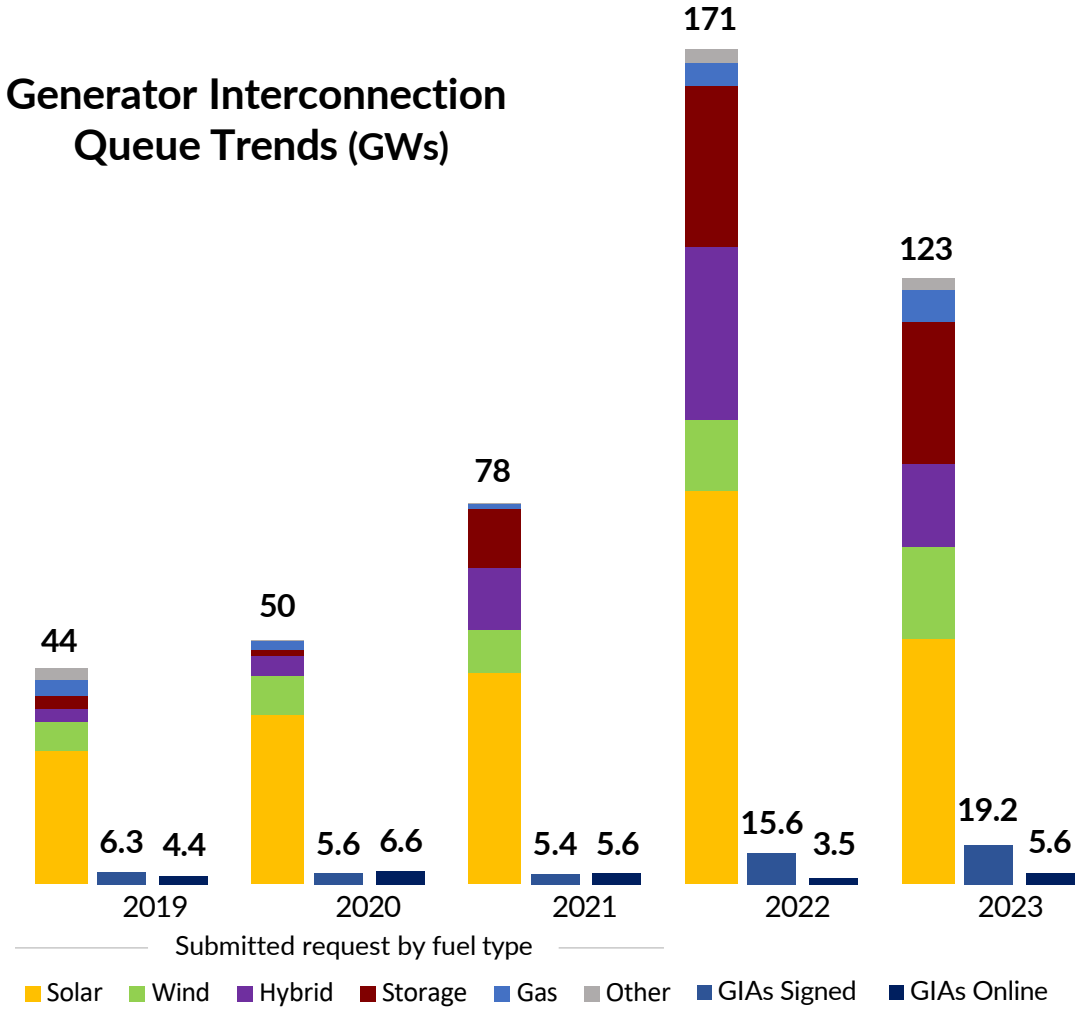
With stakeholder engagement to prioritize and sequence critical work, we expect to make significant progress on other key Market Redefinition initiatives

Examples of deliverables in 2024

Reliability Attributes	Scarcity Pricing	Reliability Metrics	Load Modifying Resource (LMR) Accreditation
<p><i>Integrate solutions identified in the Attributes Roadmap related to priority risks of system adequacy, flexibility, and system stability</i></p>	<p><i>Send the right signals about the value of energy and other products leading up to and during scarcity conditions</i></p>	<p><i>Recognize the limitations of the Loss of Load Expectation metric to determine system adequacy</i></p>	<p><i>Align accreditation with availability and account for characteristics</i></p>
<p>Deliverables</p> <ul style="list-style-type: none">• Ensure resource adequacy and energy market signals are incenting emerging needs• Require capabilities to strengthen the grid	<p>Deliverables</p> <ul style="list-style-type: none">• Present proposed changes to relevant pricing curves for stakeholder feedback• Targeting FERC filing 2024	<p>Deliverables</p> <ul style="list-style-type: none">• Evaluate new or additional risk metrics for resource adequacy assessments and their potential to improve underlying risk models	<p>Deliverables</p> <ul style="list-style-type: none">• Reliability in last stage of emergencies• Visibility in MISO Clearing Engines• Certainty for MISO and Stakeholders• Targeting FERC filing 2024

MISO reforms and Order 2023 measures to improve project readiness appear to be effective as the 2023 Queue volume decreased by 30%

Generator Interconnection Queue Trends (GWs)



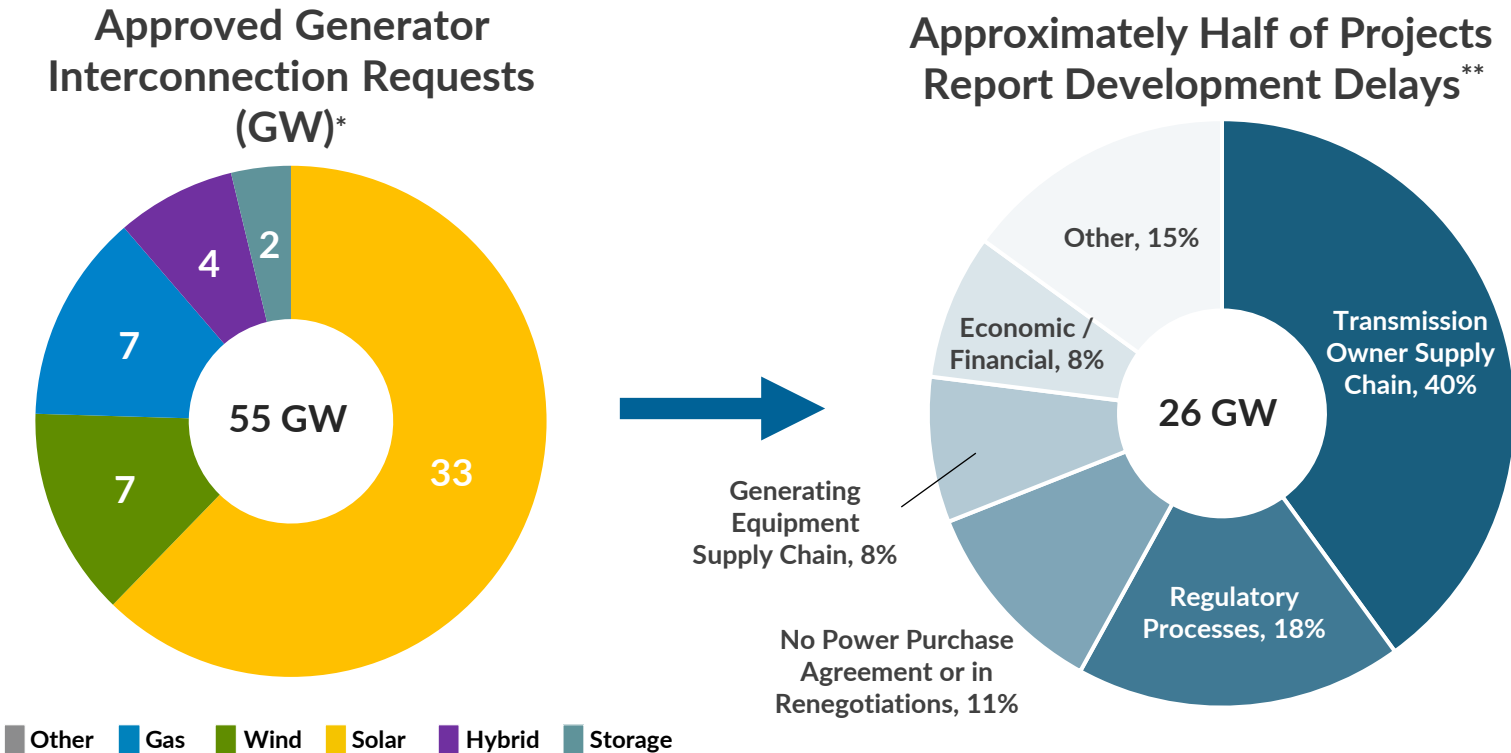
Generator Interconnection Requests

GI Requests	2023 New*	Active Queue**
Size	123 GW	349 GW
Solar	41%	49%
Storage	23%	21%
Hybrid	14%	16%
Wind	15%	11%
Gas	5%	2.5%
Other	2%	0.5%

- Reforms included withdrawal penalties and improvement to site control rules
- Signed Generator Interconnection Agreements are increasing
- Construction delays continue, with an average of ~5 GW per year of nameplate capacity coming online annually

* The 2023 Generator Interconnection Queue application cycle was deferred to April 2024
 ** Active Queue represents Generator Interconnection requests still active from prior years + 2023 New requests as of 6/12/24

While we are approving more new resources, approximately half continue to experience delays in getting online

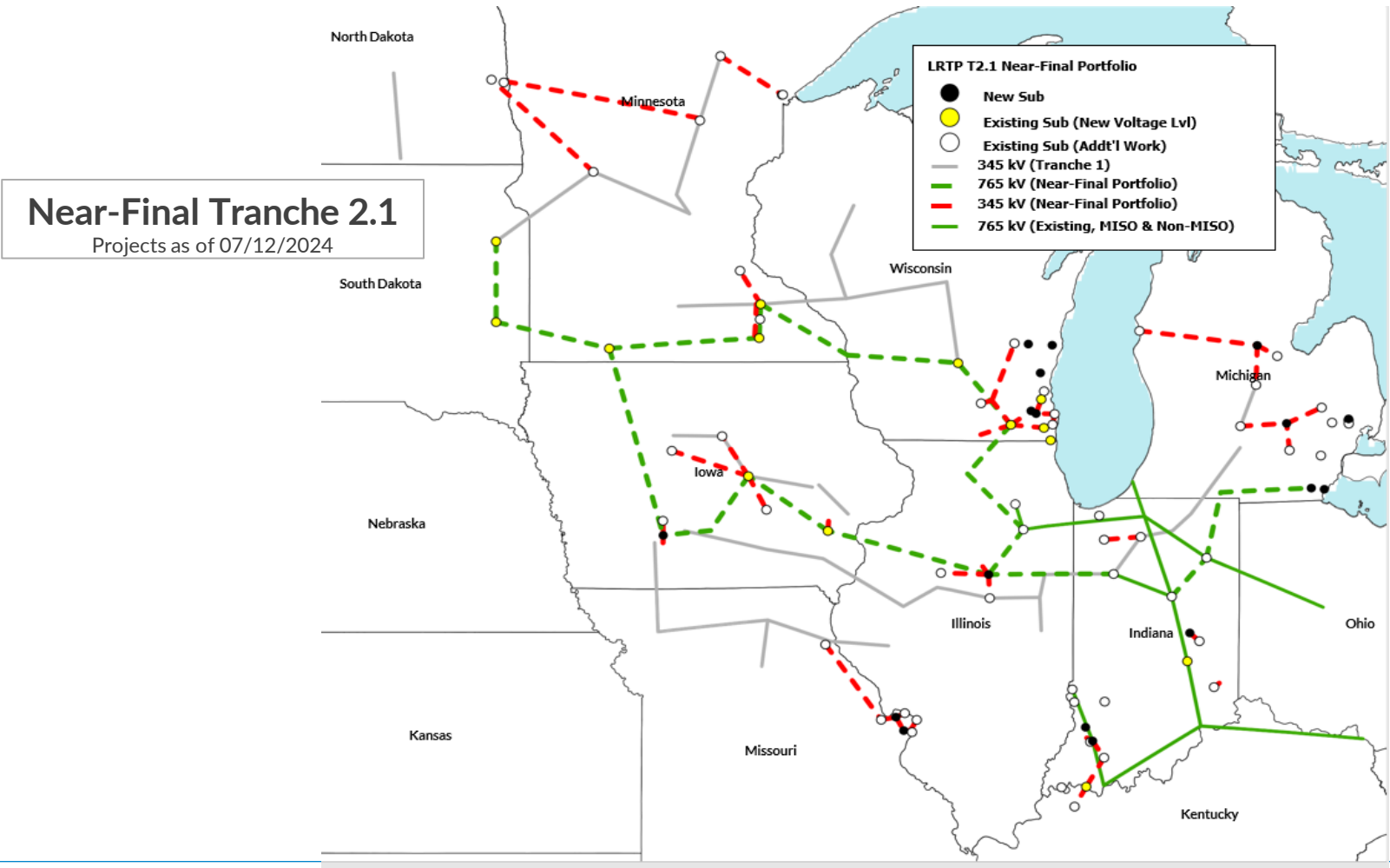


50 GW of resources approved through MISO's interconnection processes are in or awaiting construction with approximately 50% already signaling a delay

*Queue data as of September 4, 2024

** Reasons for delay based on responses from a subset of delayed projects

This work has resulted in a near-final portfolio, which will continue to be refined through business case analysis, with investment expected to be \$21 billion



MISO has been active on many fronts to improve the manageability of its Queue and provide a critical path to timely resource approvals

MISO Queue Cap Proposal	FERC Order 1920	Compliance filings completed in May FERC Order 2023 Compliance	Retirements / Replacement Process
<ul style="list-style-type: none">• Limits GW capacity in each queue cycle study• Helps MISO and neighbors manage the study process and conduct studies more quickly• Proposal specifics previously rejected by FERC will be revised and refiled in 2024	<ul style="list-style-type: none">• Compliance filings due 10 and 12 months after effective date• Requires changes to local, regional, and interregional processes• Requires engagement with states on cost allocation and selection criteria	<ul style="list-style-type: none">• Addresses queue backlogs, improves certainty and prevents undue discrimination for new technologies• Most directives are consistent with MISO reforms filed with FERC in January 2024• MISO adopted approximately 15 reforms	<ul style="list-style-type: none">• MISO improved its resource replacement process to correlate with the Attachment Y process and will continue streamlining processes as retirements accelerate

Coordinating and executing on the priorities within the Reliability Imperative is required to address challenges to reliability

RELIABILITY CHALLENGES

- Attributes needed to ensure reliability will become more scarce
- Extreme weather events are more frequent and severe
- Large single-site load additions and incremental load growth
- Fuel-assurance issues with gas pipelines and other energy infrastructure
- Supply chain and permitting issues are delaying generation projects
- Investor preferences to/not to finance new energy projects

KEY INITIATIVES¹

MARKET REDEFINITION	<ul style="list-style-type: none">• Resource Accreditation• Reliability Attributes• Pricing Reforms• Forecast Uncertainties
OPERATIONS OF THE FUTURE	<ul style="list-style-type: none">• Uncertainty & Variability• Planning & Preparedness• Situational Awareness & Critical Communications
TRANSMISSION EVOLUTION	<ul style="list-style-type: none">• Long Range Transmission Planning• Generator Interconnection• Joint Transmission Planning²
SYSTEM ENHANCEMENTS	<ul style="list-style-type: none">• Hybrid Cloud Capability• Fortify Cybersecurity• Advanced Data Analytics Capabilities

¹Partial listing of initiatives;

²Includes Joint Targeted Interconnection Queue (JTIQ)

As MISO executes on Reliability Imperative priorities, broad coordination is needed to consider all actions to support reliability and load growth

- Delaying retirements / maintaining existing fleets continues to be the best immediate lever
- Consideration for relaxed renewable / clean energy goals, providing longer glidepath, to reflect the magnitude of landscape change since many of them were implemented
- Collaboration on potential options for expediting the most critical new resource additions
- Moving LRTP Tranche 1 projects forward quickly and preparations for the same on Tranche 2.1

2024 FALL RELIABILITY SUMMIT

Brian Thiry, Director Entity Engagement and External Affairs

Michelle Cross, Manager External Affairs

September 18, 2024



RELIABILITY FIRST

NERC STANDARDS UPDATE

LATRICE HARKNESS

Director of Engineering, NERC



NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Critical Infrastructure Protection

NERC Overview and Project 2016-02 Revisions Update

Latrice Harkness, Director of Engineering
Fall Reliability and Security Summit
September 18, 2024

RELIABILITY | RESILIENCE | SECURITY

- Standards are one part of a holistic approach to Reliability
- Other essential NERC functions:
 - Registering and Certifying entities
 - Engineering analysis of past performance and assessments of future risks
 - System Monitoring and Event Analysis
 - NERC Alerts, Lessons Learned
 - Reliability Guidelines
 - Technical Reference Material
 - System Operator certification and training
 - Compliance Monitoring and Enforcement
 - Electricity Information Sharing and Analysis Center (E-ISAC)
 - AND MORE!



- Maintain consistent vigilance and information sharing
 - Build good-faith relationships between entities and regulatory authorities to assure a robust security posture
 - Enforcing compliance can be an effective tool but the goal is to assure a reliable, resilient, and secure electric grid
- Analyze known threat vectors, events, and reported incidents
 - Evaluate potential impacts from exposed threats (e.g., SHAMOON, Solarwinds, attack on Metcalf substation)
- Encourage proactive over reactive mindsets and behaviors



- Critical Infrastructure Protection Reliability Standards
 - Includes Cyber and Physical security
 - Protects information and access to Bulk Energy System assets
- Focus on:
 - Identifying applicable assets
 - Defining physical and electronic security perimeters
 - Prioritizing assets based on potential to impact the grid (High, Medium, Low)
 - Detailing roles and responsibilities
 - Remain flexible as technology and industry practices change
- Complimentary with the NIST Cybersecurity Framework



- CIP-002: BES Cyber System Categorization
 - Categorization of assets
- CIP-003: Security Management Controls
 - Protect against compromise
- CIP-004: Personnel & Training
 - Requires security awareness training and cyber security training programs
- CIP-005: Electronic Security Perimeter(s)
 - Define and protect an ESP
- CIP-006: Physical Security of BES Cyber Systems
 - Define methods and controls for physical security plans

- **CIP-007: Systems Security Management**
 - Specifies procedures to protect BES security systems
- **CIP-008: Incident Reporting and Response Planning**
 - Assures cyber security incidents are evaluated and communicated
- **CIP-009: Recovery Plans for BES Cyber Systems**
 - Details recovery plan specifics, implementation and testing
- **CIP-010: Configuration Change Management and Vulnerability Assessments**
 - Prevent and detect unauthorized changes
- **CIP-011: Information Protection**
 - Specify information protection requirements

- CIP-012: Communications between Control Centers
 - Protection of data in transit
- CIP-013: Supply Chain Risk Management
 - Create and implement a supply chain risk management plan
- CIP-014: Physical Security
 - Assure critical facilities are protected from physical attacks



- Address the issues identified by the V5TAG as well as directives from Federal Energy Regulatory Commission (FERC) Order Nos. 822 and 843.
 - The proposed revisions in the eleven CIP Reliability Standards and associated new and revised Glossary terms enable entities to securely use virtualized technologies for BES Cyber Systems.

- New terms – Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI)
- SCI vs. “All-in”
- CIP-010 for dynamic environments
- CIP-005 and Zero Trust models
- Interactive Remote ACCESS to non-routable (serial) BCA/BCS

- Electronic Security Perimeter is a security model rather than only a network topology-based perimeter, enabling entities to use a “Zero Trust” model, for example.
- Developing terms such as “Shared Cyber Infrastructure” and “Management Interface” to address risks, for example, by preventing use of “mixed trust”, where virtual machines of varying impact levels share the same central processing units, among other components, and the occurrence of “side channel” attacks where virtual systems executing on the same hardware could affect one another⁷.
- Applying certain CIP requirements and protections to Shared Cyber Infrastructure as an Applicable System.
- Broadening change management requirements by focusing requirements on a security objective of controlling the implementation of intended changes to software or settings that could weaken certain cyber security controls rather than only permitting a baseline configuration.

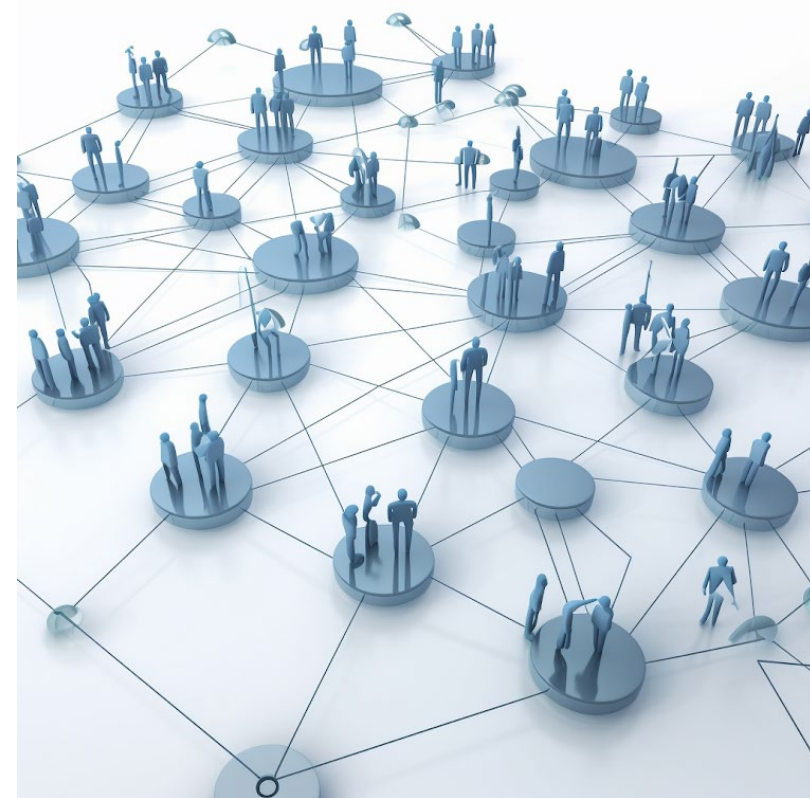
- As part of a V5 TAG-identified issue, the proposed revisions clarify that CIP-005 requirements will apply if: (1) a medium or high impact BES Cyber System only has non-routable connectivity (i.e., serial) but is subsequently converted to routable protocol; and (2) a remote user can still gain Interactive Remote Access to the BES Cyber System.

- CIP Exceptional Circumstance
 - The Project 2016-02 drafting team reviewed which requirements were most appropriate for CIP Exceptional Circumstances, which entities may declare during certain, defined emergencies to stop complying with particular CIP standards requirements in the interest of supporting reliability.
- Incorporation of CIP-002-5.1a Interpretation
 - The proposed revisions incorporate the CIP-002-5.1a interpretation regarding “shared BES Cyber Systems” by clarifying that each “discrete” shared BES Cyber System meets medium impact rating 2.1 in Attachment 1 to CIP-002-7.
- Technical Feasibility Exception
 - The proposed revisions replace language that triggers the use of the Technical Feasibility Exception procedure in the NERC Rules of Procedure Appendix 4D with the term “per system capability” that requires entities to document limits to a system but not engage in the Appendix 4D procedure.

- Impart a degree of “future proofing” to the CIP Reliability Standards to respond to the fast-changing pace in technology
- Option to use “Zero Trust” security model
- Broadens change management requirements to security objectives

- 2021-03 CIP-002
 - Impact rating criteria enhancements
- 2022-05 Modifications to CIP-008 Reporting Threshold
 - Reporting threshold refinement
- 2023-04 Modifications to CIP-003
 - Mitigating the risk of a coordinated attacks on low impact facilities
- 2023-06 CIP-014 Risk Assessment Refinement
 - Adjustments to physical security risk assessments

- Areas of focus – largest threats
 - Increasing networking and communication protocols
 - Virtualization
 - Web-based services and third-party applications
 - Distributed and increasing quantity of threat vectors (e.g., data storage, energy resources, remote access)
 - Digital supply chain





Questions and Answers

THE SANDBOX OF RELIABILITY, RISK AND COMPLIANCE

JASON THORNTON

Principal Technical Auditor, RF
Operations & Planning
Compliance Monitoring



RELIABILITY FIRST

THE SANDBOX

RELIABILITY, RISK, AND COMPLIANCE

Jason Thornton, Principal Technical Auditor,
Operations & Planning Compliance
Monitoring, RF

2024 Fall Reliability & Security Summit



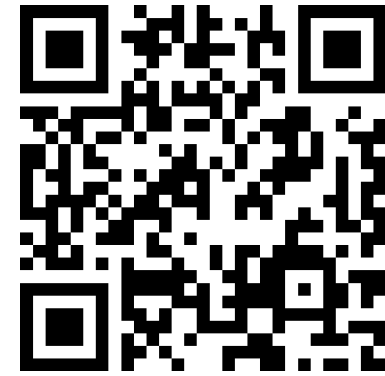
RELIABILITY FIRST

AGENDA

- LOOKING BACK
- KEY MOMENTS OF CHANGE
- THE SANDBOX CONCEPT
- RELIABILITY, RISK, AND COMPLIANCE
- FLORIDA EVENT
- CLOSING REMARKS

THE LAST 30 YEARS

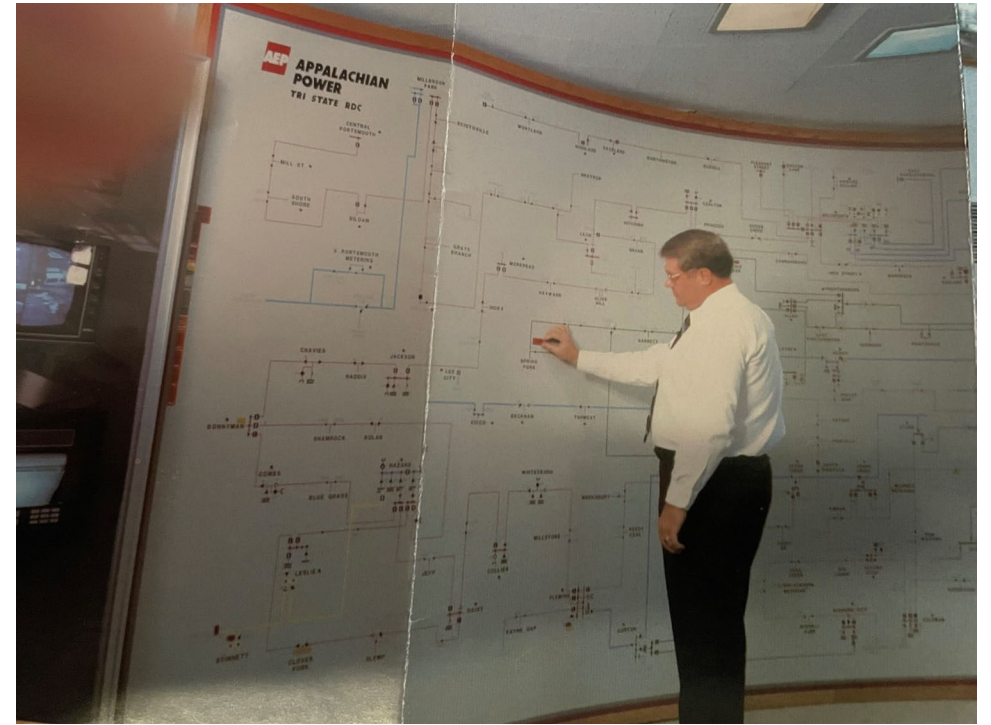
- Energy Policy Act of 1992
- Deregulation
- Competition
- Energy Crisis
- ENRON
- FERC Order 888
- No Conduit Rules
- FERC Order 679
- OASIS
- FERC Order 1000
- Required NERC Certification
- Enforceable NERC Standards
- Energy Policy Act of 2005
- Major Storm Events
- FERC Order 2000 RTOs/ISOs
- Separation of Business Units
- Regional Entities
- SCADA
- Communication Advances
- 2003 Blackout
- IPPs - Peaker Plants
- IBR (Wind/Solar)
- Transmission Growth
- Capital Investment Incentives
- EPA Requirements
- Transmission Service
- Electromechanical Relays
- Cold Weather Events



Slido.com
#RFSummit24

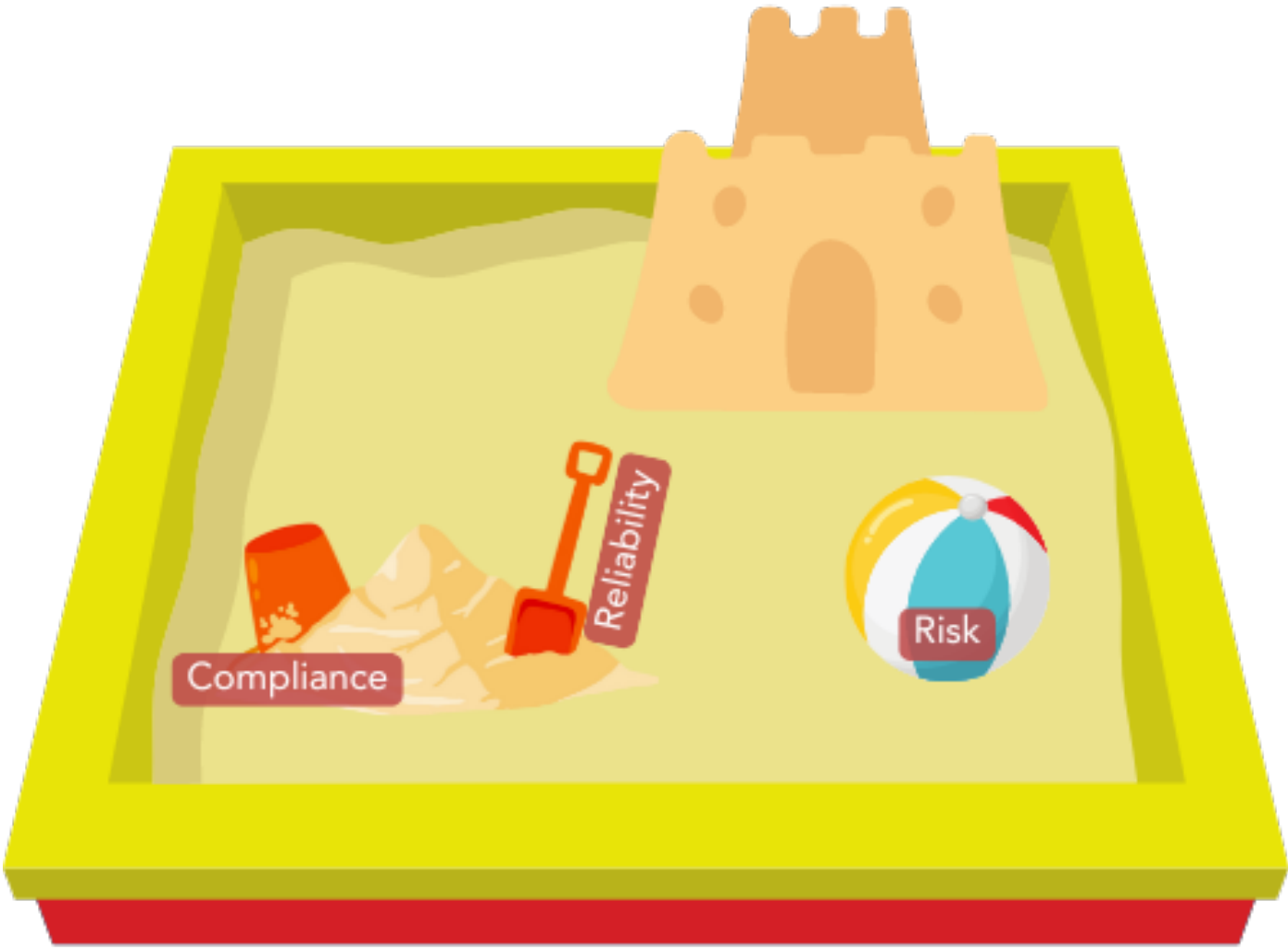
SYSTEM OPERATOR - KEY MOMENTS

- Competition/separation of generation and transmission - 1992
- Everybody wanted to be like ENRON, until 2001
- Creation of RTOs/ISOs - 2000s
- NERC Operator Certification Requirement - 2002
- Aug. 14, 2003 - Swan Dive Day
- Regional Entities created (Energy Policy Act) - 2005
- Enforceable NERC Reliability Standards - 2007
- Coal plant retirements begin - 2010s
- FERC Order 1000 - 2011



1994 AEP Tri State RDC Brochure

THE SANDBOX



RISK - RELIABILITY - COMPLIANCE

HOW DO THEY PLAY TOGETHER

Which statement(s) seem(s) correct?

- Without compliance, risk increases and reliability decreases.
- If risk didn't exist, there would be no compliance.
- Reliability is removing risk.
- Compliance reduces risk and increases reliability.
- Reliability principles are the basis for the NERC Reliability Standards.

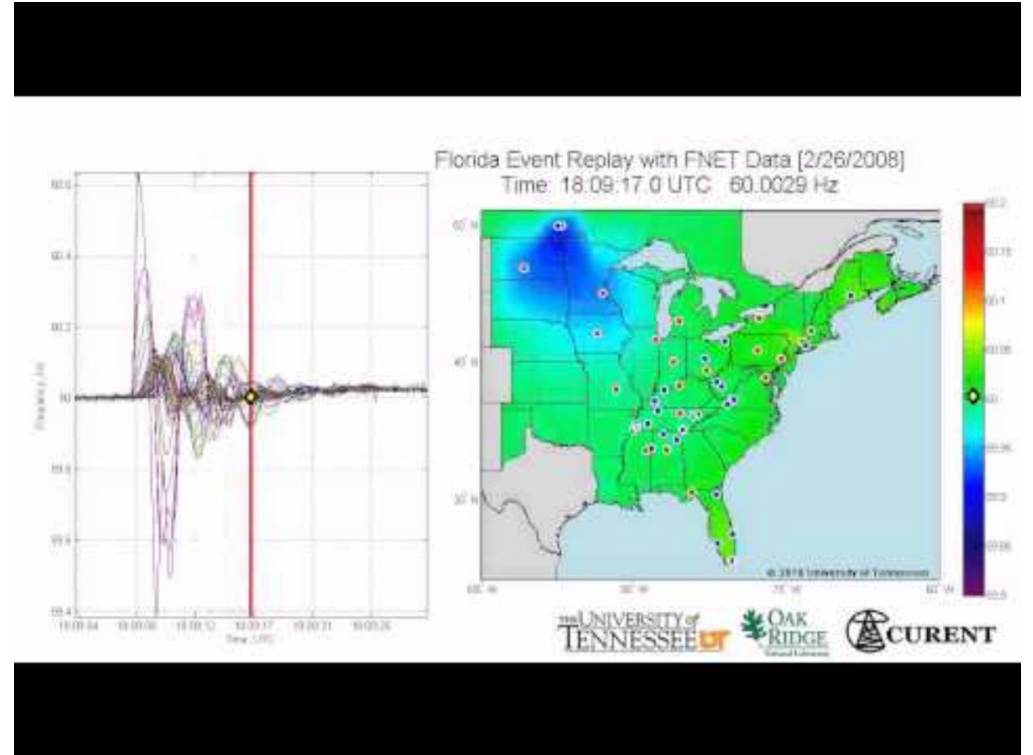
THINK ABOUT IT

What changed or is changing in compliance due to these events?

- Aug. 14, 2003 Northeast Blackout - (training, awareness, vegetation)
- Florida Blackout 2008 - (inadequate protection measures, assessments, communication)
- Cold weather events (preparedness, planning, definitions of cold weather)
- Generation retirements
- Inverter-based resources

FLORIDA EVENT (DEEPER DIVE)

- Protection Systems Disabled (Primary and Backup)
 - 22 Transmission Lines
 - 4300 MW of Generation
 - 3500 MW of Customer Load
- NERC Standards
 - BAL, COM, EOP, PER, PRC, TOP, and TPL
- \$25M Settlement
 - Additional \$350,000 for RC Function (IRO and COM)



<https://youtu.be/bdBB4byrZ6U?si=MDhBzSWCLV-xg0Kc>

RESULT OF RULING

- Ruling resulted in greater industry awareness around the risk of reduced and inadequate protection for relay systems.
- Regardless of the violation language, that did not identify a specific requirement(s), entities were taking actions to avoid the risk. A reliability precedence was established even though protection systems were not specifically addressed in this capacity in the Reliability Standards.
 - Would actions be taken by other utilities if the entity was not found at fault?
 - Did the \$25M settlement help drive attention to this matter?

CHANGES TO NERC STANDARDS

As a result of the Florida Blackout in 2008, the following standards and requirements were created or modified:

- .

WHAT DID WE LEARN

Risk



- Risk is not necessarily always known, so there is never zero risk.
- However, risk can be managed and controlled if you follow the guidance provided to minimize risk.

Reliability



- Reliability is an expected state that we manage through good policies, continuous improvement, evaluation of risk, and ultimately adherence to what are known as best practices.

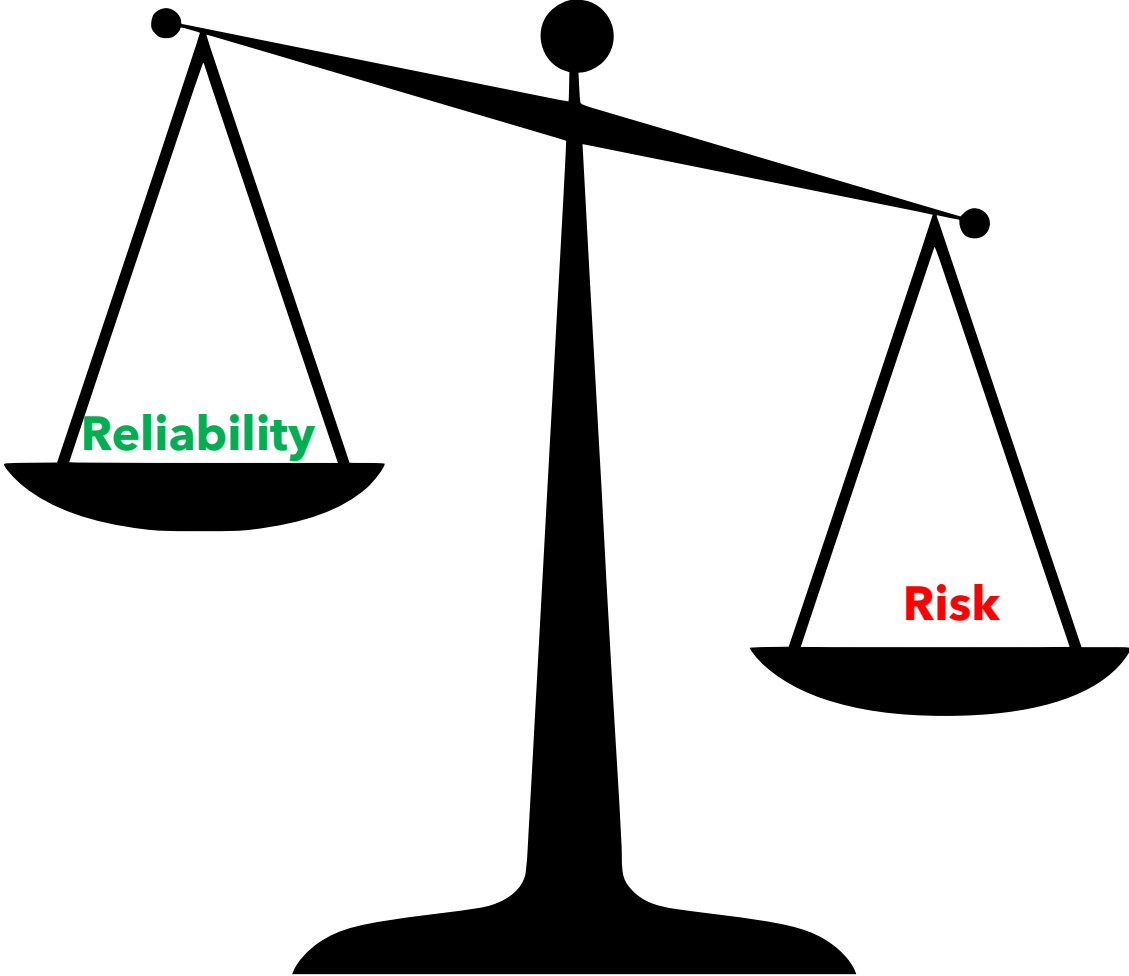
Compliance



- Compliance does not cover every risk and is meant as sound guidance for reliability.
- A proactive approach to compliance is needed to reduce risk and improve reliability.

COMPLIANCE - RISK - RELIABILITY

WHAT DOES IT REALLY LOOK LIKE



COMPLIANCE

HOW DO WE MANAGE RISK

CONTROLS

CULTURE



RISK

What risks do we face? What keeps you up at night?

Overall Risks

- Event Response & Resilience
- Situational Awareness
- Planning & Modeling
- Cyber and Physical Security
- Protection System Misoperations
- Human Performance
- Vegetation Management
- Extreme Weather

CIP ERO Identified Risk Themes

- Latent vulnerabilities
- Insufficient commitment to low impact CIP programs
- Shortages of labor and skillsets
- Performance drift



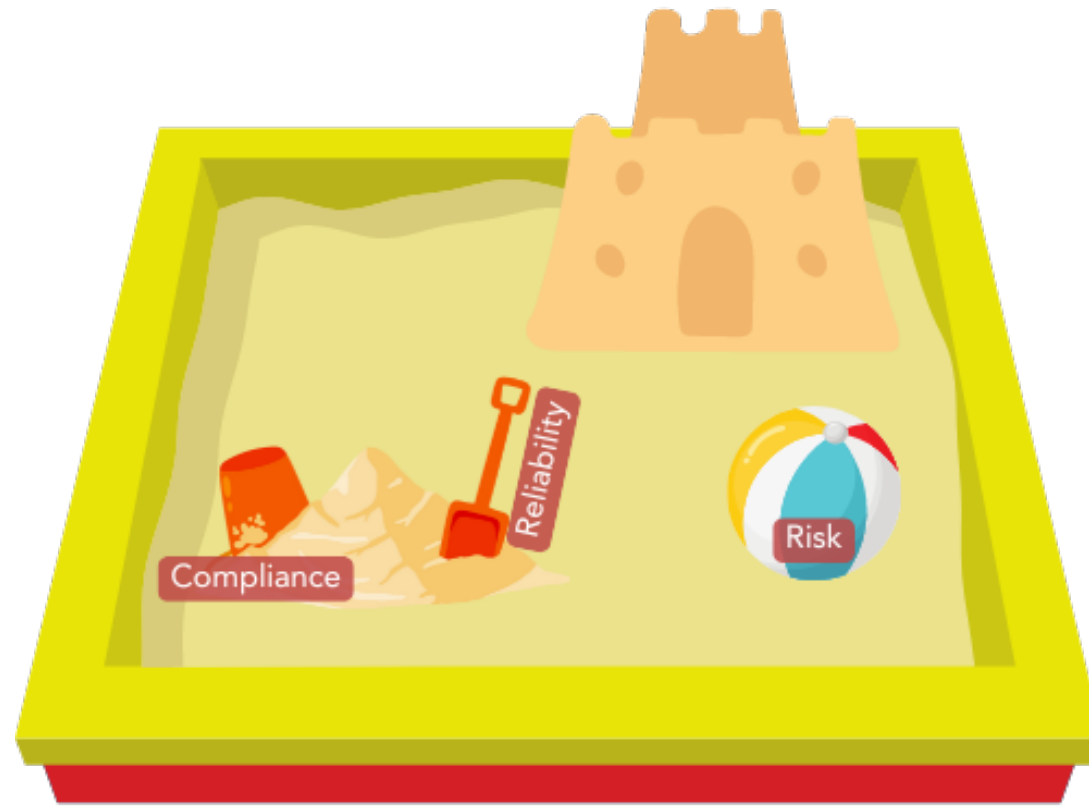
Slido.com
#RFSummit24

RELIABILITY

- Understanding risk before it becomes a risk and setting up controls to manage those risks.
- Operating within the boundaries established by the Reliability Standards.
- Being proactive and sharing ideas and concerns.
- Setting a tone that supports all activities that contribute to reliability.
- Being a partner to those in front, behind, up, down, and sideways while making sure your actions are supportive.
- Being active!! Take advantage of resources, join teams and committees, and make a difference. We need you!

COMPLIANCE

Something you want to do or something you have to do?





QUESTIONS & ANSWERS

Jason Thornton

Jason.Thornton@RFirst.org